Report of the
Defense Science Board
2008 Summer Study on

Capability Surprise
Volume II: Supporting Papers

January 2010

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense. The 2008 Summer Study on Capability Surprise completed its information-gathering in August 2008.

This report is unclassified and cleared for public release.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR: Under Secretary of Defense for Acquisition, Technology and Logistics

SUBJECT: Final Report of the Defense Science Board 2008 Summer Study on Capability Surprise

I am pleased to forward the final report of the Defense Science Board 2008 Summer Study on Capability Surprise. This report offers important considerations for the Department of Defense in response to future threats to our nation's security.

This study concerns itself with the matter of capability surprise, which can arise from many sources—scientific breakthrough, rapid fielding, operational innovation. It considers two fundamental kinds of surprises: 1) those specific few, that because of their unique characteristics and impact, the nation should be anticipating—referred to as "known surprises"; and 2) those that arise unexpectedly out of a myriad of other possibilities, seemingly without warning—the "surprising surprises." The premise of the study is that surprise cannot be eliminated, but it can—and must—be managed.

Today, the Department of Defense and the nation are not adequately prepared to manage surprise—to reduce the potential for its occurrence or to respond rapidly and appropriately, should it occur. Thus, the study's recommendations focus on improving critical processes and implementing new ones: scanning and assessment, red teaming and exercising, rapid fielding, strategic intelligence, and integration and management.

I endorse all of the study's recommendations and encourage you to forward the report to the Secretary of Defense.

Paul G. Kaminski

Dr. Paul G. Kaminski
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR: Chairman, Defense Science Board

SUBJECT: Final Report of the Defense Science Board 2008 Summer Study on Capability Surprise

The instability and cultural complexities in today's world, the breadth of security challenges, and the capability not only of states, but of non-states and extremists to "make really bad things happen" create an environment in which the potential for surprise has reached new levels. As of yet the nation has found no simple form of deterrence to deal with this complex environment. Thus, we as a nation must be prepared to deal with surprise in new ways.

This study addresses the issue of capability surprise—what it is, why it happens, what can be done to reduce the potential for its occurrence, and how the Department of Defense and the nation can be better prepared to respond appropriately.

Capability surprise can spring from many sources: scientific breakthrough in the laboratory, rapid fielding of a known technology, or new operational use of an existing capability or technology. A review of many surprises that occurred over the past century suggests that surprises tend to fall into two major categories:

- **"Known" surprises**—those few that the United States should have known were coming, but for which it did not adequately prepare. For this category of surprise, the potential and evidence are clear; the effects are potentially catastrophic; and dealing with them is difficult, costly, and sometimes counter-cultural. We specifically include space, cyber, and nuclear in this category today. We might also have included bio, but with a focus on threats to military operations, we chose not to.
- **"Surprising" surprises**—those many that the nation might have known about or at least anticipated, but which were buried among hundreds or thousands of other possibilities. In this case, the evidence and consequences are less clear, the possibilities are many, and the nation cannot afford to pursue them all.

In both cases, the biggest issue is not a failure to envision events that may be surprising. It is a failure to decide which ones to act upon, and to what degree. That failure results, at least partially, from the fact that there is no systematic mechanism in place within DOD or the interagency to help decide which events to act on aggressively, which to treat to a lesser degree, and which to ignore, at least for the time being. Thus, the principle recommendations of this study focus on developing the approaches and the talent to better manage surprise—to prevent it from happening or, should surprise occur, to be in a position to rapidly mitigate its consequences.

The Department must take several important steps in order to more effectively manage capability surprise:

1. **Integration and management** of surprise at a high enough level to affect senior decision making**.** Secretary of Defense formally establish a Capability, Assessment, Warning and Response Office (CAWRO) to provide DOD senior

leadership with timely assessment and warning of potentially high-risk adversary capabilities with options and recommendations for addressing them.

2. **Red teaming** as the norm instead of the exception. Secretary of Defense direct the use of red teaming throughout DOD by developing and employing best practice guides, intellectual focus in professional military education, and more aggressive use of red teams in exercises. The Secretary should also lead by example and establish a strategic-level red team to challenge and inform national security and top level defense policies and strategies.

3. **Rapid fielding** that is truly rapid and can be effectively employed when the circumstances warrant. The Under Secretary of Defense for Acquisition, Technology, and Logistics establish a standing Rapid Capability Fielding Office (RCFO) to improve DOD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs.

4. Pointed improvements in **"strategic" intelligence.** The Director, National Intelligence Warning Office, in the National Intelligence Council, provide adequate resources for "strategic intelligence" and establish a cell within the CAWRO. The cell and its interaction with the CAWRO support multiple objectives —to better monitor adversary intent and capabilities over time, to help focus collection efforts on key activity signatures, and to continuously update key adversary vulnerabilities that the nation can exploit. Improvements are also needed in the area of detecting foreign denial and deception.

5. For **known surprises**, the Secretary of Defense establish a formal mechanism to ensure Department progress in addressing the limited number of most critical threats. Focus is needed on ongoing assessments; operational exercises, games, and red teaming; and improving the nation's abilities to deter, detect, prevent, mitigate, fight through, and use appropriate offensive measures.

For surprise management to be successful, however, there needs to be support from leadership at the highest levels—a recurring theme of this study. Emphasis should be placed on encouraging alternative viewpoints, requiring broad risk/opportunity assessment, integrating and synthesizing, and enhancing knowledge through cross-domain teaming. Without such leadership, the tendency will be to maintain the status quo … and the nation will be seriously surprised.

Dr. Miriam John
Co-Chair

Mr. Robert Stein
Co-Chair

Table of Contents

Preface

The 2008 Defense Science Board summer study addresses the issue of capability surprise—what it is, why it happens, what can be done to reduce the potential for its occurrence, and how to better prepare the Department of Defense (DOD) and the nation to respond appropriately.

Surprise is not a new phenomenon and can spring from many sources. This study examined three domains that characterize the manner in which adversaries most often create capability surprise.

1. **Operational innovation.** Adversaries develop a new and unanticipated operational capability by employing new tactics, techniques, and procedures rather than new materiel or weapons. Often this type of surprise emerges when existing equipment is used in ways that were not anticipated or for objectives that were not foreseen. The nation missed the signs, often contained in written doctrine or live exercises, indicating the potential or lacked the imagination to think "out of the box."

2. **Adaptation of new technology.** Adversaries employ new, previously unused technology and adapt it to their needs. The United States is unaware of the new technology (which is not a common occurrence) or did not imagine (or more likely did not believe) that an adversary would employ the new technology against our nation.

3. **Rapid fielding.** Adversaries develop a new military capability using existing systems or technology, but transition it to a fielded capability much more quickly than anticipated. The United States may be aware of the development but is surprised by how quickly it emerges in the field—often assuming that adversary processes to field new systems mirror the lengthy ones in DOD.

Study members convened in separate panels to examine each of these potential sources of surprise. Through the lens of its surprise domain, each panel crafted recommendations aimed at improving U.S. capabilities to prevent, respond to, and/or mitigate the consequences of surprise.

The results of this study are presented in two volumes. Volume 1, the Main Report, presents a synthesized view of the findings and recommendations of the full study membership. This volume, Volume 2, Supporting Papers, reports self-contained discussions by each of the study's three principal panels—Operations, Technology, and Transition and Fielding—and provides considerably more detail on many aspects of the material presented in Volume 1.

While the detailed findings and recommendations provided Volume 2 do not in all cases represent the synthesized view of the full summer study membership, the fundamental issues contained in each of the panel reports are largely in agreement with the synthesized view. The three panels reporting herein agree on the need:

- To establish a high-level organization, the Capability Assessment, Warning, and Response Office, to provide DOD senior leadership with a mechanism to manage surprise.
- To establish an organization within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics to aid in rapid transition and fielding of new war fighting capabilities that will improve DOD's ability to address priority surprise capability gaps and support urgent war fighter needs. This organization should be formed through the consolidation/elimination of the numerous, and largely suboptimal, "rapid" organizations already existing in the Department.
- For establishing red teaming as the norm instead of the exception and for improving strategic intelligence—two areas essential to enhancing the Department's surprise management capabilities.
- For leadership support at the highest levels if the Department and the nation are to be successful at managing surprise.

Where some of the recommendations in this volume may differ from those in Volume 1, the differences lie in the implementation details. And although we, as chairs of this study, support the implementation paths found in Volume 1, we nevertheless feel that the alternative implementation approaches described in this volume are both viable and important to report.

Part One.
Operational Innovation

Chapter 1-1. Introduction

This report, prepared by the Operations Panel of the Defense Science Board 2008 Summer Study on Capability Surprise, provides richer detail about the impact of surprise on military operations, past historical examples of surprise, and other areas addressed in the study. The summer study was charged with examining the many facets of capability surprise that an adversary can inflict on the United States. Specifically, the study considered three different domains in which capability surprise can occur: (1) surprise in the laboratory, (2) surprise during transition from concept to fielded product, and (3) surprise introduced by the unconventional or unforeseen use of an existing capability. The Operations Panel focused on historical examples of "surprise" in an attempt to derive insights that may be useful for minimizing capability surprise in the future.

Although most people possess an intuitive grasp of the concept of surprise, a single definition, particularly in the context of national security and military operations, is elusive, but likely includes:[1]

- to cause to feel wonder, **astonishment**, or amazement because of something **unanticipated**
- to come upon or discover **suddenly** and **unexpectedly**
- to make an **unexpected** assault on
- to elicit or bring out **suddenly** or **without warning**
- a completely **unexpected** occurrence, appearance, or statement
- an assault made **without warning**
- to strike the enemy at a time, place, manner for which he is **unprepared**
- **astonishment** felt when something totally **unexpected** happens
- the discovery of a reality that was previously **hidden**
- (act of) surprise is in the hands of our enemies … but the effects of surprise are in our hands

As Peter Schwartz and Doug Randall of the Monitor Group noted in their February 2008 article, "Ahead of the Curve: Anticipating Strategic Surprise," a

1. http://dictionary.reference.com/browse/surprise

strategic surprise has three key elements that differentiate it from the run-of-the-mill surprises that are common in today's complex world:

- It has an important impact on an organization or country.
- Because it challenges the conventional wisdom—"the official future," as we like to say—it is difficult to convince others to believe that the surprise is even possible.
- It is hard to imagine what can be done in response.

Thus, strategic surprises can be categorized as those patterns of events that, if they were to occur, would make a big difference to the future, would force decision-makers to challenge their own assumptions, and would require tough decisions. As Mr. Schwartz notes, "Strategic surprises usually reshape the rules of competition. The question then becomes: What are the assets needed to win, and when do strengths become weaknesses, and vice versa? Vantage point also matters; something can be a strategic surprise for one company or country but not for another, because an event's impact may be felt differently."

In the final analysis, however, surprise cannot be avoided. It will happen. While the act of surprising the United States might reside in the hands of an enemy, many of the immediate effects remain in our own hands. Therefore, it is critical that the nation maintain the capacity within its institutions and decision-making processes to rapidly react and adapt to surprises at all levels. Because of America's inherent culture of pragmatic adaptability, its economic capacity, and military and social stability (staying power), our nation tends to handle most surprises well at the tactical and operational levels. The nation has also, on certain occasions, recognized the potential of existential surprise and committed resources as "insurance" against the catastrophic. Perhaps the most compelling example of a successful policy to mitigate capability surprise was the evolving U.S. strategy for nuclear deterrence during the Cold War.

However, we as a nation do not routinely deal well with strategic or existential surprise for which planning and flexibility are important. We do not understand the true nature of the conflict. We do not question initial assumptions. We are not clear about strategic goals and objectives, and are even less clear in understanding our adversaries' mindset. We are poor at planning and integrating across all elements of national power. We are slow to appreciate and adapt to changing situations. And we do not do a good job of assessing impact beyond the immediate effects and/or compellingly conveying it to senior leaders.

The conduct of the war in Iraq in recent years has demonstrated many of these deficiencies. The United States entered into that conflict without a clear idea of its true nature and without questioning its basic assumptions. Consequently, the nation soon found itself surprised that the situation failed to develop along the strategic lines first envisioned. Our "system" did not transmit information about the changing nature of the conflict to the highest national command authorities in a manner that was sufficiently compelling to force change. A large component of this problem stemmed from the reluctance of senior political and military leaders to question their initial assumptions until well into the conflict. Consequently, they did not consider new strategies or policies that were more appropriate to the true situation.

Most surprises do not occur within a single domain. Rather, they appear across domains or at their intersection. For example, nations or their military forces are rarely surprised by the existence of a new technology. More often, surprise is brought about either by the use of some preexisting technology in a novel way or by an anticipated technology being developed in an unexpectedly short time. Moreover, small or lower levels of surprise can have dramatically disproportionate effects if they are misunderstood or not managed appropriately. Thus, the perceived inability of the United States to cope with the tactical surprise presented by the widespread use of improvised explosive devices (IEDs) in Iraq affected public support for the war. In essence, tactical surprise was creating a strategic impact with far-reaching policy implications—and we as a nation were surprised by the connection between the two. Going one step further, it is even conceivable that strategic surprise can transform itself into an existential crisis if national leadership fails to understand and control its potential.

The remainder of the Operations Panel report examines in further detail "operational" surprise—where an existing capability is used in an innovative or unforeseen manner. Chapter 1-2 begins with an assessment of the emerging security environment and its challenges. The report then turns, in Chapter 1-3, to a discussion of modern cases of operational surprise. Chapters 1-4 and 1-5 examine two areas of surprise in depth: cyber surprise and surprise in space. The report concludes with a discussion about creating operational surprise.

Chapter 1-2. The Emerging Security Environment

Looking back over the past twenty years, the changes that have occurred in the security environment are significant in both numbers and scope. And these changes presage more to come in the future. The capabilities available to the U.S. armed forces to defend the nation—ranging from precision strike to stealth technologies—are substantial and increasingly sophisticated. Unfortunately, those who wish the United States harm or bare us ill will are also the beneficiaries of a growing arsenal of capabilities. The playing field in conventional warfare will likely still favor the United States and its allies for some time into the future—considering our resiliency and the depth and breadth of our collective capabilities. However, affordability, technological availability, and cultural and ethical mindsets that are very different from those of our nation have allowed potential adversaries to bring a different game to the field—one that is more favorable to them and the dimensions of which will likely not be fully known to the United States. As a result, the nation can and will be surprised. Yet, even as surprise cannot be avoided, the ability to anticipate, prepare, mitigate, adapt, and even reverse surprise is not only possible, but paramount to the security of our nation and its people.

Compelling Changes

Of the many changes that have and will continue to occur in the national security environment, perhaps the most compelling are greater international integration and interconnectivity, major power dynamics, new and novel technologies and techniques, the rise of non-state players who possess the ability to inflict significant harm, and demographic change. The sections that follow discuss each of these factors in turn.

Greater International Integration and Interconnectivity

Globalization will remain the most influential trend through the next decade. Increasing interconnectivity and interdependence will likely sustain world economic growth and raise world living standards in the aggregate. At the same time, while much of the world will reap the benefits of globalization, those states and regions that are left behind will face deepening stagnation, political instability, cultural alienation, and the potential for societal and individual radicalization.

Advances in communications and transportation remain core enablers of this era of globalization, surpassing previous periods. The scope of players (multinational corporations and former "backwater" nations) and the speed of action (transactions and travel within a day or less vice a week or more) accrue to a far broader and diverse group. These compressed timescales place a much higher premium on planning and preparations, and the United States will need to rely more heavily on partners to help stay ahead of the pace and to ensure effectiveness and avoid over-stretching U.S. capabilities.

Even where globalization is perceived to be progressing, exposure to—and integration into—a broader global community can change the nature and stability of societies by weakening existing norms and creating unforeseen and unpredictable situations. In broad terms, some Middle East regimes continue to reject global integration, fearing challenges to their authority. Additionally, much of sub-Saharan Africa lacks the infrastructure and leadership to connect globally. Even where connections have been made in trade and commerce, the relationship is uneven and, in a growing number of cases, detrimental. Local merchants cannot compete or the local labor force is ill-equipped to participate. A growing backlash to globalization is not only visible in the developing world but within segments of the populations in Europe and North America.

Major Power Dynamics

Major power conflict remains unlikely in the near term, although competition for resources and influence are points of increasing friction.

The emergence of China, India, and Brazil, with their growing economic power and expectations, is challenging and transforming traditional 20th century institutions and practices. Additionally, despite its demographic crisis, Russian influence will likely increase because of its upsurge in oil wealth. Additionally, one should expect an increasingly aggressive Russian security posture, resulting from Russian concerns about encirclement from the West and a craving for respect from the international community. From a Russian perspective, enlargement of the North Atlantic Treaty Organization (NATO) and placing missile defenses in former satellite states are not surprising causes for concern.

China's growing global footprint is also an increasingly significant consideration for U.S. security interests and its strategy for regional engagement. China's presence is most prominent in Africa and Latin America, where China is winning contracts for mineral extraction through attractive aid packages to develop transportation and communications infrastructures. China now ranks close to both the United States and Europe in total trade with Africa and is pursuing significant investment and trade opportunities in Latin America.

In 1991, Chinese direct investment in Africa was less than five million dollars a year. By 1994, it was around $25 million and by 1999 just short of $100 million. Just seven years later, He Wenping, director of the African Studies division in the Chinese Academy of Social Sciences, stated that direct Chinese investment in Africa reached $1.25 billion in 2006.[2] China's trade with Africa has also grown sharply, from $11 billion in 2000 to an estimated $50 billion in 2006. Most of the trade is in Africa's favor, through export of oil, minerals, and other natural resources.[3]

Trade between China and Brazil hit $12 billion (U.S.) in the first half of 2007, a year-on-year increase of 30.1 percent, according to statistics from the Chinese Ministry of Commerce. Brazil is now one of China's main suppliers of iron ore and soybeans, while China is a fast-growing supplier of electronic goods and components to Brazil.[4]

---

2. "China in Africa: It's Still the Governance Stupid," *Foreign Policy in Focus*, March 9, 2007.
3. *China Ups the Ante in Africa*, Center for Strategic and International Studies, December 2006.
4. "Call for Greater Chinese Investment in Brazil," *China Daily*, December 28, 2007.

Demand for energy will remain a critical factor in international relations as emerging economies become increasingly dependent on fuel growth, particularly in China and India. Distribution has become a significant challenge, with energy production further away from consumers.

Growth in the demand for energy and basic materials (such as steel and copper) is moving from developed to developing countries, principally in Asia. For example, demand for oil in China and India will nearly double from 2003 to 2020, to 15.4 million barrels a day. Asia's oil consumption will approach that of the United States—currently the world's largest consumer—by the end of that period.[5]

The complexity and interconnectedness of the majority of regional security issues demand broader strategic collaboration. However, the willingness of existing and emergent world powers to collectively seek solutions is uncertain. That willingness in recent experience has come haltingly and the trend looks to continue. The future relevance of institutions like NATO and the United Nations may require their transformation.

New and Novel Technology and Techniques

Rapid advances in basic and applied technology, combined with a global community predisposed to share knowledge, is dramatically increasing the availability of sophisticated technologies. The use and misuse of new capabilities will continue to stimulate the global economy and improve quality of life, but may also increasingly challenge U.S. defense and security capabilities. Major surprise from the unanticipated use of increasingly available technologies is becoming more and more likely. For the foreseeable future, investment and research in new technologies around the world will be driven primarily by the private sector—and not just in the United States and Europe, but in Korea and Japan as well. Centers of science and technology excellence are emerging in China, India, Singapore, and Brazil.

Worldwide research and development (R&D) expenditures, unadjusted for inflation, rose from $377 billion in 1990 to $810 billion

5. "Global Trends in Energy," *The McKinsey Quarterly*, February 2007.

in 2003, the last year of available data. The Organisation for Economic Cooperation and Development (OECD) countries' share dropped from an estimated 93 percent to 84 percent of the total over the period. Governments around the world are increasing their R&D funding to support the development of high-technology industries. However, private R&D support has often expanded more rapidly, leading to a declining share of government support in total R&D in many countries. The relative decline in the United States had been very steep—the federal government share fell from 48 percent in 1990 to a low of 26 percent in 2001. Changes after September 11, 2001, largely in defense and national security R&D, raised the bar to 31 percent in 2004. Whether or not that increase will be sustained is an open question. In the European Union, the government share diminished from 41 percent in 1990 to 34 percent in 2001.[6]

In many cases, technology advances will amplify other trends. Computing has already enabled developments in biotechnology—in bioinformatics and modeling of protein folding, for example. Quantum computing will no doubt allow even greater sophistication and speed in these developments. The absorption of technology is also an issue. Societal norms and political leadership will govern the incorporation of technological change in global societies, with profound economic, social, political, and military implications.

Foreign R&D advances have also resulted in new or novel weapons and weapons systems. Not surprisingly, many of these programs are focused on countering U.S. capabilities, particularly in the areas of precision, access, and information. Potential adversaries will seek a range of low-cost options that they hope will level at least part of the playing field with the United States—or, even better, secure asymmetric advantages.

Non-State Players

Irregular challenges will ebb and flow for the United States in the coming decade, but they are generally on a steady upward trend line. Of particular note is the increased potential influence of individuals and

6. National Science Foundation, Division of Science Resources Statistics, *Science and Engineering Indicators*, 2006.

groups. Non-state actors have greater access than ever before to a range of capabilities to threaten or inflict considerable damage. While the ability of one individual to make a significant impact is hardly new, the scope, nature, and potential damage from such impacts has grown exponentially in the past two decades. The ubiquitous availability of computers, the Internet, and mobile communications technologies provide adversaries with the capability to instantaneously transfer information, as well as collaborate with like-minded individuals anywhere in the world. Dual-use equipment, materials, and technologies are proliferating around the world through a web of commercial ventures that are nearly impossible to track, much less to control, to prevent their use in malicious ways. Perhaps the most troubling aspects of the empowered individual or group are the ability to remain anonymous, to mask intent and capability, and to act in a manner that is seemingly, at least to the United States, irrational.

Organized crime, militants, and terrorist groups now exploit the prime enablers of globalization, taking full advantage of advanced communications and transportation. Criminal groups rely not only on the ungoverned spaces of weak states for refuge and basing, but also feed off the fragility and vulnerability of emerging economies. Through illicit networks, ready cash flows, and willing recruits, they can quickly constitute and command an armed force that rivals or even surpasses the capability of many of the law enforcement and security forces in areas from Latin America to Central Asia.

These non-state actors are often more flexible, more willing to accept greater risk, and, therefore, able to act more rapidly than traditional state actors. They are characterized by horizontal and flat organizational structures. Furthermore, their sustainment is centered far more on the cause or purpose of the group, than who is in charge or which physical assets or territory they possess. Thus, removal of leaders or damage to infrastructure does not constitute the same vulnerability as it does in a nation state. Finally, fringe elements of terrorist groups often will act independently, because they do not require central direction. These highly decentralized, cellular adversaries challenge the United States' ability to attribute threats and plan effective interdiction strategies.

Demographic Change

Global demographic trends will have far-reaching consequences for U.S. interests. Some of these trends are well underway and are reshaping the global landscape. Most developed countries' birth rates are below the population replacement level and their populations are aging. Thus, there will likely be increasing demands on the contracting labor force to fund social programs. For some states, such as those in Western Europe, these funding demands will increase pressures to cut military budgets.

For the first time in history, a majority of the world's population lives in cities. As that trend continues, urban infrastructure and services may have difficulty meeting increased demands. Furthermore, urbanization tends to concentrate precisely in the demographic groups most inclined to violence. This seems particularly true in the Middle East and Africa. Some urban areas already lack legitimate governance and security. That said, ungoverned rural areas, like those in Pakistan, are still problematic.

Security Environment Challenges

The Flow of Information

The increased speed and dissemination of information and disinformation has already fostered a more complex security operating environment. Situational awareness favors the agile, adaptable, and knowledgeable. Additionally, mass media, in all its forms, has proven to be both beneficial and detrimental. While the rapid distribution of information on events aids in understanding the operational picture, it also contributes to background noise, confusion, and misrepresentation of the actual events. Furthermore, the rapid flow of information has a noticeable effect on decision-making processes. Leaders are often driven by the need to "get ahead of the breaking story."

The ability to hide information has also taken on greater importance in a world with instant communications. Steganography, combined with encryption techniques, embed hidden communications within digitized images, providing secure communications channels "in plain view."

Social networking and virtual worlds are emerging venues for communications. Their use is largely being defined by the next generation. Older generations are casual observers at best with limited or passive participation. This informal "news" network has exacerbated the content and trust issues of more formal venues. Information, accurate or inaccurate, is spreading rapidly through the public domain and causing reaction.

The challenge for U.S. operations now and into the future is in maintaining a common operating picture of the battle space, deciphering what is real, uncovering what is missing, and making and communicating decisions above the "noise."

The Nature of Governance

Over the coming decade, demographic, economic, environmental, and cultural changes will place increasing pressure on the world's governments. Some will fail. Weak states and ungoverned spaces will challenge regional institutions to enforce security and will complicate the ability to take meaningful, enduring action. Areas of the world experiencing chronic state failure will evolve with emergent networks of local, informal governance, such as in Afghanistan and Somalia. Both reverted to indigenous systems lacking conventional legal or moral constraints. The potentially destabilizing effects of poor governance and the lack of rule of law will affect U.S. security interests and complicate engagement strategies.

Globalization Dependency

While taking part in globalized trade has economic benefits, a host of potential downsides accrue as well. National and international commercial infrastructures, such as financial institutions, ports, and rail lines, are subject to attack. Additionally, the reality that much manufacturing is internationalized and the origin of suppliers is not always known can create vulnerabilities. Similarly, the United States is increasingly dependent on services provided from offshore; this represents yet another potential source of vulnerability.

Chapter 1-3. Modern Cases of Capability Surprise

There is an old saying, "you don't know where you're going if you don't know where you've been." In this spirit, the Operations Panel examined historical cases of "surprise," paying particular attention to determining why the surprise occurred. Consideration was also given to understanding the consequences of surprise and mitigation and stabilization strategies, with the goal of capturing insight that might help the nation avoid surprise in the future and inflict surprise on others.

Categories and Causes of Surprise

There are countless cases of surprise, but for the purposes of this study, the focus was narrowed to relatively modern examples, dating from World War II to the present. The selection of case studies also endeavored to identify examples of surprise in three principal categories: cases where the United States was surprised; cases where the United States inflicted surprise; and non-U.S. examples of surprise. The fourteen cases examined (Table 1-1), while by no means comprehensive, provide ample evidence of why surprise has occurred in the past. These case studies proved useful as a means to gain insight into why surprise—both good and bad—happens, and what impact it has had.

Surprise from New Capabilities

New capabilities are often at the heart of surprise. It is important to note, however, that while technology is often the engine that powers a new capability, the existence of the technology, in and of itself, is not a surprise. In all of the cases examined during this study, the technologies were known. The source of surprise came from the innovative use of the technologies, the timing of the introduction of the capability, or the unexpected implication of the capability.

Table 1-1. Summary of Historical Cases of Surprise

Historical Case	Causes	Responses	Institutional Reactions	Overall Lessons
Battle of the Beams in World War II (beginning 1940)	▪ Recruit the cream of the nation's talent, and give them authority. (Contrary to Freeman Dyson's experience in the Royal Air Force.) ▪ Precisely targeted intelligence collection	▪ Escalating series of operations, feeding success on success	▪ Scientific intelligence established in Ministry of Defense and MI6 (United Kingdom's Secret Intelligence Service)	▪ Small amounts of world-class talent, at the right place and time, authorized to act, can have decisive effects on a conflict
Pearl Harbor (1941)	▪ Leadership failure ▪ Tactical failures ▪ Failed to imagine form of attack ▪ Communications problems among organizations	▪ Tactical command, control, communication and intelligence (C3I) improvements	▪ None	▪ Surprise during transition-to-war can have especially severe consequences
A-Bomb World War II Termination (1945)	▪ Multiple order-of-magnitude increase in destructiveness ▪ Inconceivable to victim	▪ Japanese psychological shock, and rapid surrender ▪ Disorientation and disorder in U.S. defense community	▪ National labs ▪ Atomic agencies ▪ Redefined armed	▪ Inconceivable surprises can break even the toughest national will ▪ Such advantages are fleeting
Berlin Air Lift (1948–1949)	▪ Under-estimated Allied resolve and capability	▪ Harassment: search-lights, buzzing, electronic warfare ▪ Psychological operations: food offers ▪ U.S. exploited victory as enduring symbol of charity and resolve: dropping candy-bars; "Ich bin ein Berliner"	▪ USSR divided Germany ▪ U.S. escalated capabilities for global mobility and supply	▪ Value of non-combat, "soft" military capabilities ▪ Parable for development of similar 21st century capabilities: cyber defense; etc. ▪ Importance of protecting mobility from cyber threats and basing denial
Sputnik Launch (1957)	▪ Failure to inform leadership and public of possibility ▪ Collateral event can embody wider fears (Red Scare; nukes)	▪ Rally the nation to science education and advances ▪ Explorer & Corona programs	▪ Defense Advanced Research Projects Agency (DARPA), National Aero-nautics and Space Administration (NASA) ▪ National Defense Education Act ▪ Greater U.S.–U.K. cooperation	▪ Difficulty of science and technology (S&T) warning—especially in closed states (same story in opposite direction during bomber and missile gaps) ▪ Cost of technical arrogance
Tet Offensive (1968)	▪ Assumed enemy wouldn't launch non-viable attack ▪ Didn't properly manage public expectations (especially in light of Communist persistence vs. French) ▪ First televised war	▪ Decisively won tactical engagements ▪ Ineffective civil affairs and media mgmt	▪ Denial/dissonance in leadership; sense of unfairness ("but we won") ▪ Avoid insurgency ▪ Powell doctrine	▪ Sometimes the enemy gets lucky (e.g., strategic success blooms from the seeds of operational failure)

Table 1-1. Summary of Historical Cases of Surprise (continued)

Historical Case	Causes	Responses	Institutional Reactions	Overall Lessons
Bombing of Marine Corps Barracks in Beirut (1983)	▪ Did not view ourselves as combatants (vs. peace-keepers) ▪ Measures to robustly defend vs. charging trucks were not well-understood	▪ Withdrawal ▪ Ineffective retaliation	▪ Began a long series of force protection improvements to foreign posts ▪ Trough in balance between remote and close-access intelligence collection investments	▪ Bombing is frequently a successful, low-tech attack ▪ Defensive red teams may reveal weaknesses ▪ Defensive measures vs. bombings are absolutely necessary, but not sufficient
Operations Desert Shield/Desert Storm (1990–1991)	▪ Cohesion of coalition, with basing and transit advantages ▪ Public perception of "just war" and U.S. interests at stake ▪ Unveiling of stealth and precision guided munitions ▪ No opportunity for natural or urban cover or concealment of targets ▪ Effective U.S. deception effort ▪ Virtually all Iraqi forces technically inferior to U.S. ▪ Modest Iraq capability for *mobile* defense, especially under unprecedented air attack ▪ Incompetent Iraqi leadership; inert force after initial invasion	▪ EMCON (emissions control) suicide + precision guided munitions attacks → unit isolation and collapse ▪ Premature termination due to ground forces out-running communications, and one-sided casualties	▪ Most adversaries went mobile, underground, clandestine, and/or nuclear ▪ People's Republic of China and Russia began re-building armed forces ▪ Investment shift toward "more" precision strike and C3I at expense of other capabilities	▪ "Perfect storm" for surprise: incompetent victim + technical superiority + effective deception + effective national leadership ▪ Competitors will attempt to rectify gross imbalance in capabilities
Attacks on World Trade Center (1993)	▪ False assumption: U.S. = sanctuary ▪ Law enforcement dominated by forensic approaches unsuited to counter-terrorism ▪ Counter-intelligence and counter-terrorism then viewed as niche activity in FBI	▪ Forensic analysis and attack attribution ▪ Improved intelligence collection, law enforcement agency communications, and network analysis led to roll up of Abdel-Rahmen cell ▪ Misplaced confidence in forensic action	▪ No recognition that U.S. homeland was being targeted ▪ Anti-Terrorism Antiterrorism and Effective Death Penalty Act of 1996	▪ Drawing the wrong lessons from a "win" can create the next "loss" (i.e., 9/11)

Table 1-1. Summary of Historical Cases of Surprise (continued)

Historical Case	Causes	Responses	Institutional Reactions	Overall Lessons
September 11 Attacks (2001)	▪ Attack fell into seam between foreign intelligence and domestic law enforcement ▪ Law enforcement dominated by forensic approaches unsuited to counter-terrorism	▪ Passengers on 3rd aircraft appear to have understood and foiled final attack ▪ First responder efforts ▪ Offensive campaign vs. Al-Qaeda	▪ Centralized intelligence and homeland security oversight and budgeting ▪ Massive increase in intelligence & special operations forces investments ▪ Relax legal strictures on Intelligence Community – law enforcement agency seam ▪ Intelligence Community information sharing/ collaboration initiatives ▪ Finally fixed commercial aircraft security after 40 years of hijackings	▪ Must remedy structural weakness in national security community inherited from Cold War (Will likely learn this lesson again after "Cyber Pearl Harbor")
Operation Enduring Freedom, Afghanistan (2001)	▪ Assumed enemy behavior ▪ Ignorance of military capability ▪ Diplomatic isolation ▪ Fighting "last war"	▪ Flee ▪ Revert to non-state operations	▪ U.S.: none ▪ Al-Qaeda: franchising	▪ U.S. entirely capable of inflicting operational surprise, absent revolutionary technology
Titan Rain Cyber Attacks (beginning 2003)	▪ Persistent unwillingness to balance security vs. cost and functionality in C3 / information technology system design ▪ Unable to discriminate valid user behavior from exploitation ▪ No *visible* evidence of damage = no learning	▪ Monitored and characterized ongoing attacks ▪ Technical attribution measures ▪ Instances where leadership "killed the messenger" in an attempt to cover up the penetrations	▪ Continued state of denial within DOD (and federal government and business leadership) ▪ Joint Task Force on Computer Network Defense → computer network operations; global network operations ▪ Increased Defense-wide Information Assurance Program (DIAP) and DARPA investment ▪ Beginnings of offense-defense integration	▪ We are repeating history: Crecy, Portiers, Agincourt ▪ Will require courageous leadership at Secretary of Defense and President level to change course

Table 1-1. Summary of Historical Cases of Surprise (continued)

Historical Case	Causes	Responses	Institutional Reactions	Overall Lessons
Use of Improvised Explosive Devices in Operation Iraqi Freedom (beginning 2003)	▪ National leadership failure ▪ Violate public trust and expectations ▪ Poor planning ▪ Didn't foresee political imperative to persist in opposing U.S. objectives ▪ Symmetric, conventional initial response	▪ Tactical mitigation efforts (jamming, armore, training, etc.) ▪ Shift to Iraqi security forces ▪ Attack on clan networks ▪ Created 2nd order problems	▪ Resolve political deadlock in country ▪ Tighter Intelligence Community–DOD integration ▪ More robust technical support to operational forces	▪ Loss of public trust is lethal to war effort ▪ Poor planning is deadly ▪ New weapons cannot necessarily be "solved" – but need not dominate outcome ▪ Misguided responses can worsen the surprise
Israel and Hezbollah in the Second Lebanon War (2006)	▪ Poor planning and decision-making ▪ Miscalculated ability of intelligence, surveillance, and reconnaissance to localize highly distributed, low-end threat ▪ Discounted impact of anti-tank guided missiles (ATGMs) and IEDs on armor ▪ Discounted civil impact of unguided rockets ▪ Poor tactical force training	▪ Increased weight of effort (too late) ▪ Ineffective civil affairs and media management ▪ Ineffective management of international efforts to terminate fight before Hezbollah could be eliminated	▪ National inquiry, with corrective measures ongoing	▪ Under-estimating enemy can produce surprise ▪ Imbalance in force capabilities can disable high-end force engaging a covert opponent ▪ Incompetent leadership can decisively tip outcome, even in strong vs. weak conflicts

The German blitzkrieg in World War II is a good example of a new capability arising out of the imaginative use of existing technologies. Great Britain, France, Germany, the Soviet Union, and the United States all developed and experimented with airplanes, tanks, and radios between the two world wars; only Germany successfully combined them into a new operational capability before World War II.

In the case of Sputnik, surprise was caused by the first employment of a new technology—although the potential was known. The fact that the Soviet Union was first into space shocked the American public. It was inconceivable that the Russians could launch into space before America. As a result, Sputnik initially caused a large measure of national hysteria. The knowledge that the rocket that carried Sputnik into orbit could also carry weapons into the United States was cause for alarm. More importantly, Sputnik was a warning that the United States was falling behind the Soviet Union in scientific areas in which the United States had long believed it was dominant. In the immediate aftermath of its launch, however, Sputnik served as an example of how surprise can be exploited or reversed. The United States undertook a massive campaign to boost science education (National Defense Education Act) and created governmental organizations, such as the Advanced Research Projects Agency (ARPA) (later to add the word "Defense" and become the Defense Advanced Research Projects Agency (DARPA)) and the National Aeronautics and Space Administration (NASA), to increase U.S. space and science capabilities.

Dropping the atomic bomb on the Japanese is another example of surprise that resulted from the first use of a new capability. The potential of nuclear fission was not a surprise to the scientific community. Indeed the U.S. program was originally motivated by the knowledge that the Germans were well on their way to creating a fission weapon. The first use by the United States against Japan, however, created sufficient shock within the Japanese state to force its unconditional surrender within days. This capitulation was largely unimaginable by those in control of Japan before Hiroshima. Indeed, more destruction and death had been—and would have been—visited on Japan with conventional weapons than by the atomic bombs. Eventually, others eliminated the U.S. atomic monopoly by developing

their own weapons. Ironically, the atomic surprise for the United States was how rapidly the Soviet Union developed these weapons.

All capability surprise is not, however, necessarily limited to offensive weapons or actions. Here, the "soft power" example of the Berlin Air Lift is instructive. During the Berlin Air Lift, the United States used its asymmetric air transport capabilities to thwart the Soviet attempt—by blockading ground access to Berlin—to essentially starve all of Berlin into their sphere of influence. The Soviets could not imagine that the United States could move sufficient food and fuel into West Berlin by air to sustain the population. The air lift did just that and, as a result, Soviet policy was frustrated. Furthermore, the United States realized from this experience the importance of strategic lift and escalated efforts to improve its capabilities for global mobility and logistics. A few years later, when interest in the strategic movement of troops and supplies around the United States became a concern of the Eisenhower Administration, these lessons were applied to the creation of the Interstate Highway System.

Asymmetric Capabilities Can Surprise Dominant Militaries

History also shows that potential adversaries will adapt existing technologies in ways that surprise stronger opponents and nullify their supposed advantages—the so-called asymmetric threats. This was the case with Hezbollah versus Israel in the 2006 Second Lebanon War. In that war, the Tel Aviv military put its faith in stand-off attack by artillery and air power, enabled by intelligence, surveillance, and reconnaissance (ISR), as the primary means to coerce Hezbollah into returning Israeli captives and to stop rocket attacks on Israel. This was the prevailing Israeli view about how future wars would be fought. During the conflict, it became evident that finding and destroying Hezbollah's short-range rockets was not feasible with airpower and ISR. It was not until late in the conflict that Tel Aviv turned to its ground forces to defeat Hezbollah. Unfortunately for the Israeli Defense Forces, the Army had neglected high-intensity combined arms training, focusing almost exclusively on low-intensity and counterinsurgency threats from the Palestinians. They had become highly capable in this

kind of warfare during the years countering the intifadas at the expense of more conventional ground warfare.

Hezbollah's use of widely available anti-tank guided missiles, mines, and IEDs stymied what most believed until then to be the best Army in the Middle East. Thus, the Second Lebanon War was a two-edged surprise to Israel: their assumptions about future warfare were wrong and their resulting capabilities were inadequate to confound the Hezbollah threat. The Israeli Defense Forces fell victim to a classic military "surprise"—fighting the "last war," or fighting the war you "want" as opposed to the "war you might get."

The United States faced a similar situation at the end of Operation Iraqi Freedom (OIF) with the onset of an insurgency and the proliferation of IEDs. Quite simply, imagining and attempting to prepare for the possibility of an insurgency was not allowed by key high-level civilian leaders in the United States. Thus, best case assumptions about conditions in postwar Iraq were never tested, and contingency planning for what might replace the vacuum caused by the removal of Saddam Hussein and his regime, and how best to do it, was not done.

As the insurgency began, the enemy began employing IEDs, particularly against unarmored support vehicles. Initially, much of the explosives used in the IEDs came from unsecured Iraqi ammunition dumps. IEDs are not a new phenomenon—they caused significant problems for U.S. operations during the Vietnam War. However, the scale, scope, and extensive use of these weapons surprised the Department of Defense (DOD) when they began causing significant casualties in Iraq.

The U.S. vulnerability to IEDs, as well as the broader issue of unanticipated casualties, caused significant credibility problems among the public and the body politic. Crash programs for body armor and mine resistant vehicles resulted and a new organization was created, initially the Joint Improvised Explosive Device Defeat Task Force (JIEDDTF) and later the Joint Improvised Explosive Device Defeat Organization (JIEDDO). The continuing surprise, however, has been the ability of the insurgent to adapt the IED triggering attack modes and operational employment faster than the United States can develop countermeasures or defeat mechanisms. Indeed, there may be no

technical solution to eliminating IEDs. A key lesson from OIF is that countering the insurgency, not just the insurgent's weapons, is the surest route to success. This was pointed out in the Defense Science Board's 2006 IED study, but the findings and recommendations to this effect were not widely endorsed by the political leadership at the time.[7] Planning for and resourcing post-major combat operations are necessary precursors to a successful strategy that precludes the emergence of an insurgency.

All this is not to say the United States cannot itself inflict asymmetric capability surprise. Operation Enduring Freedom, which caused the collapse of the Taliban in Afghanistan and put Al Qaeda on the run, was a major surprise to the enemies of the United States. More distant examples include the awakening of the U.S. "sleeping giant" after Pearl Harbor; the development and employment of the atomic bomb; the ability of the United States to project power in a host of contingencies since World War II; and the integration of stealth, speed, and precision attack in Operations Desert Shield and Desert Storm, OIF, and elsewhere.

Operational and Tactical Surprises Can Have Strategic and Political Effects

Understanding the fundamental nature of war and the adversary one is fighting (Clausetwitz's main dictum) is a precondition to understanding the affects of surprise in the battlefield on national policy. Indeed, Clausewitz's oft-evoked notions about strategy, politics, and the will of the people are still very instructive. Key to maintaining the public's support for military operations is their understanding of the stakes involved and their confidence in the political-military leadership. Surprise in military operations for which the public is not prepared can often have disastrous strategic consequences and unhinge policy—despite short-term positive tactical or operational outcomes in the wake of the surprise. Two examples make the point: (1) in Vietnam in the

7. *Defense Science Board Task Force on Improvised Explosive Devices* (IED), 2006 (classified). The bottom line of the findings was that the IED cannot be effectively countered by playing defense at the tactical level. It requires an integrated strategic campaign with components of offense, defense, strategic communication, and intelligence. The primary issue is counterinsurgency.

wake of the Tet Offensive; and (2) in Lebanon after the bombing of the Marine barracks.

The 1968 Tet Offensive during the Vietnam War is perhaps the most famous historical U.S. example of "winning a battle, but losing the war." Although U.S. and South Vietnamese forces decimated the communist attackers after their initial attacks, the very fact of the offensive stunned the U.S. public. Quite simply, U.S. political-military leaders had spun the war to the American people, feeding them a never-ending stream of glowing reports on the successful progress of the war. The Tet Offensive, although it resulted in a crushing tactical defeat of the communists in the field, came as a strategic surprise to the American people and was the beginning of the end of the U.S. presence in Vietnam—and the South Vietnamese government.

Tactical reverses can also have strategic implications. The 1983 bombing of the Marine barracks in Beirut, Lebanon is such a case. That a terrorist attack could cause large numbers of casualties among highly competent U.S. forces was a traumatic surprise to the American public. Preventing this enemy action was eminently possible—if its possibility had been anticipated. In the aftermath of the bombing President Ronald Reagan withdrew U.S. forces from Lebanon.

Thus, when there is dissonance between what the government says will happen and what does happen, even surprise at the operational and tactical levels, can affect strategy and policy. More recently, the United States came close to a similar juncture in Iraq during the early years of OIF. The American public had been told that Iraqi civilians would be "cheering in the streets," that there would be no insurgency, and that a U.S. military presence would overwhelm what little resistance remained. Yet, the daily toll of IEDs on American troops began to grow and continue without interruption or any seeming solution. Once again, a tactical weapon was having a strategic impact.

New Organizations and Talent Can Create Significant Operational Capabilities to Create or Mitigate Surprise

This historical review also highlighted the fact that there are cases in which focused government attention on a problem and the recruitment of talent can make a significant contribution to creating surprise or mitigating its effects. The Manhattan Project that created the atomic bomb is one well-known example where the talents of a nation were mobilized to a specific purpose. The Manhattan project was also an enormous organizational endeavor, demanding unparalleled resources and program management. Furthermore, the Manhattan Project was something that the private sector of the day could not have accomplished—the U.S. government was fundamental to creating the atomic bomb.

Injecting special, non-traditional expertise into government or military institutions can also create new capabilities. This was the case in Great Britain during World War II. In 1939, the British government realized that their intelligence services were not sufficient to the tasks that would confront them in modern war. Consequently, they undertook the large-scale recruitment of highly talented individuals, *e.g.*, scientists and mathematicians, to their intelligence services. Code-breaking and scientific intelligence made major contributions to understanding Nazi intentions and capabilities, thus averting surprise and confounding German operations. The formation of the 10th fleet in 1942 to counter German offensive operations in the North Atlantic is another example of a special, nontraditional organization (a "fleet" with no ships and only 50 permanently assigned personnel) that had a game-changing effect on a previously unsolvable problem.

JIEDDO is a current example of an institutional response by DOD to the problem of IEDs in Iraq and Afghanistan. Here, again, an organization was created and tasked to marshal the necessary talent and bring together under one roof many different disciplines in order to solve a specific problem that exceeded the capacity of existing institutions to resolve. It is highly unlikely that an extra-governmental organization, in and of itself, could have dealt with this challenge. Contemporary and

future challenges in the realms of cyber, space, nuclear, biological, and others will surely demand similar leadership by the United States.

Stabilizing after Surprise is Critical

The ability of a nation to stabilize after surprise is a critical capability. After the attack on Pearl Harbor the United States was able to accelerate the industrial and manpower mobilizations already begun prior to the attack. In retrospect, the scale and scope of this mobilization was staggering in both manpower—particularly in the Army (Table 1-2)—and materiel (Table 1-3).

Table 1-2. U.S. Army Manpower Mobilization, World War II[8]

Year	Officers	Enlisted	Total
1940	18,326	250,697	269,023
1941	99,536	1,362,779	1,462,315
1945	891,663	7,376,295	8,267,958

Table 1-3. U.S. Materiel Mobilization in World War II, 1941–1945[9]

Military Aircraft	293,066
Tanks	88,079
Motor Transport Vehicles	3,200,436

The comparative advantage U.S. industrial mobilization provided was especially stark when comparing the massive U.S. shipbuilding effort to that of the Japanese (Table 1-4).

8. Russell F. Weigley, *History of the United States Army* (Bloomington: Indiana University Press, 1984), p. 599.
9. W. F. Craven and J. L. Cate, eds. *The Army Air Forces In World War II: Volume VI Men and Planes* (Chicago: University of Chicago Press, 1955; reprint, Washington, D.C.: Office of Air Force History, 1983), p. 352; and Harry C. Thomson and Lida Mayo, *The Ordnance Department: Procurement and Supply* (Washington, D.C.: United States Army Center of Military History, 1960; reprint, 1991), pp. 263, 296.

Table 1-4. U.S. and Japanese Ship Production in World War II[10]

Type	Japan as of December 1941	U.S. as of December 1941	Japan Production During War	U.S. Production During War
Battleships	10	17	2	8
Aircraft Carriers	10	8	16	141
Cruisers	36	36	9	48
Destroyers	113	171	63	349
Escorts	0	0	0	498
Submarines	63	112	167	203

It is also important to note that the United States was able to mobilize within a homeland sanctuary. American industrial sites, unlike those in Europe and Asia, were never attacked. Furthermore, after the fall of the Philippines in May 1942, the Unites States largely set the timetable for engaging the enemy: the United States took the offensive when it was ready. The first U.S. campaigns against the Japanese began in New Guinea in July 1942 and Guadalcanal in August 1942. Naval actions came earlier, with the Battle of the Coral Sea in May 1942 and Midway in June 1942.

In the European theater, the first major offensive, in North Africa, began nearly a year after Pearl Harbor in November 1942 and the U.S. Army Air Forces flew their first bombing mission against the European continent in October 1942. In many ways, American resilience and capacity were the greatest surprises of World War II. The Pearl Harbor surprise pales in comparison to the surprises of abject defeat visited on the Japanese and Germans. The key to all of this was a strong national will, a reserve capacity that could surge, and leadership.

In all the wars it has fought since World War II, the United States has had the advantages of material wealth and physical sanctuary. Actual "hot" wars—the Korean War, the Vietnam War, the two Gulf Wars, and a host of contingency operations—have always been fought

10. John Ellis, *World War II: A Statistical Survey* (New York: Facts on File, 1995), pp. 245, 280.

on the opponents' territory with expeditionary forces possessing enormous technological and materiel advantages. Nevertheless, these operations have resulted in mixed success. And, even more significant, the U.S. advantages of enjoying sanctuary and largely deciding when and where to fight appear to be eroding.

The bombing of the World Trade Center in 1993, the attacks by Al Qaeda on September 11, 2001, and Titan Rain beginning in 2003 are all indications that sanctuary from actual attack on the homeland, enjoyed by the United States for most of its history, is tenuous. Furthermore, unlike the Cold War, during which the United States faced nations that because of certain circumstances—e.g., centralized civilian leadership, known value system, vulnerable assets high on that value system—could be deterred, the ability to deter current and potential state and non-state adversaries is not certain. Thus, the determination of when and where action will happen—and surprise—is no longer the sole province of the United States.

One final lesson from World War II, Korea, and Vietnam is important: the U.S. ability to mobilize is different than it was during these earlier conflicts. The United States began conscription in September 1940, over a year before the attack on Pearl Harbor. Manpower needs in Korea and Vietnam were also met through conscription. Finally, the scale and comprehensiveness of World War II industrial mobilization is almost unimaginable today.

These two characteristics of the past U.S. strategic situation—physical isolation and immense mobilization capacity—come together in an important way that affects future U.S. resilience and its capacity to recover from surprise. Manpower, absent conscription, is a relatively fixed resource and is compounded with the reality that moving to conscription bears enormous political costs and has embedded delays even if such a decision were to be taken. Industrial mobilization, given the complexity of modern weapon systems and the globalization of U.S. manufacturing capability is also a limitation. In short, future conflicts, be they against emerging state or non-state actors, will likely be with forces and capabilities in being. Thus, the pre-war preparatory phase so vital to U.S. success and resilience in World War II, or the ability to hold the line during the Korean War, may be capabilities of the past.

Surprising One's Self is Often the Problem

There is also the very real issue of self-inflicted surprise. This can happen in many ways and several aspects are dealt with below.

Focusing on the Story One Wants

It is understandable that institutions focus their intelligence resources on the threats that are perceived to create the greatest vulnerabilities. It is also true that this focus on what is most likely to happen diverts resources from alternative assessments. Thus, ironically, one's own activity can cause surprise, particularly when intelligence appears to support the story one wants to believe. Furthermore, indicators about "the" surprise are often thought at the time to be "noise," because they do not fit or support the presumed most likely case. This is what happened in the Pearl Harbor attack. As Roberta Wohlstetter wrote in her book *Pearl Harbor: Warning and Decision*, U.S. political and military leaders did not believe Japan had the capability to attack Hawaii, and thus were focused on other possibilities.[11] Wohlstetter notes: "the very human tendency to pay attention to the signals that support current expectations about enemy behavior." She also explains the broader implications of such a focus on the most probable: "If no one is listening for signals of an attack against a highly improbable target, then it is very difficult for the signals to be heard." And viewpoints that do not conform to expectations are often not able to fight their way to the attention of policymakers because they do not comport with what they believe are the most likely cases. The dots are there, but no one sees them, much less connects them.

This inability to "connect the dots" is thus very understandable. C. V. Wedgwood explained this dilemma quite nicely: "History is lived forward, but it is written in retrospect. We know the end before we consider the beginning and we can never wholly recapture what it was like to know the beginning only."[12] Thus, retrospectively, it is easy to draw a straight line from the 9-11 attacks back to evidence that terrorists

11. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (California: Stanford University Press, 1962), p. 392.
12. C.V. Wedgwood, *William the Silent* (London: Phoenix Press, 2001), p. 35.

were taking flying lessons and that there was consideration of using airliners as weapons. On September 10, 2001, this was noise.

Surprising one's self is not, however, always simply a failure of imagination or an inability to find indicators in the noise. Often, it is a combination of the above with an institutional unwillingness to recognize the handwriting on the wall. The case of the Germans continuing to pass operational information via their Enigma machines is such an instance. The Germans failed to consider the possibility that the allies were reading their mail. The rigorous steps the allies took to safeguard the fact that they were getting Enigma intelligence were fundamental to maintaining the ULTRA secret. The Sputnik case also falls largely in this category. U.S. leadership could not imagine the Soviets would get into space first and, thus, overlooked some indicators that indeed the Soviets were on that path. This error is not unlike the one made about the ability of the Soviets to build atomic and hydrogen bombs much more quickly than believed possible. A certain degree of hubris, leading to the belief that "they can't do that" or "they wouldn't dare to do that," was a frequent underlying cause to many of the surprises this summer study examined.

Furthermore, there is the pernicious case of institutions repressing intelligence that does not support prevailing views or, even worse, spinning the intelligence to fit expectations. During the Korean War, General Douglas MacArthur's staff in Japan consistently misjudged first North Korean, and then Chinese intentions, despite having substantial intelligence that each would attack. This intelligence did not fit the "story." Similarly, there was warning before the Tet Offensive that the communists were going to attack. A number of military officers and civilian analysts held the view that post-war conditions in OIF were not going to be what the administration promoted before the invasion, but those views were suppressed from being acted upon. Similarly, the Israelis, for the most part, knew the capabilities Hezbollah possessed before the 2006 Second Lebanon War but did not fully prepare to deal with them. In each of these events, senior leaders—both political and military—deluded themselves about the downside possibilities of their actions and could not see, underestimated, or ignored their opponents' capabilities and intentions. As a consequence they were surprised.

Failing to Revisit Assumptions and no "Plan B"

Perhaps the most recent and compelling example of not revisiting assumptions is the U.S. plan for post-war Iraq in the wake of the 2003 invasion. The central assumption was that the Iraqi people would treat the coalition as liberators and that there would be a smooth transition to a stable, democratic society.

These central assumptions about Iraq were never rigorously challenged before OIF. Worse, dissenting views were suppressed. Consequently, any effort to create a "Plan B" that might be put into effect if an alternative future occurred other than that which was envisioned was soundly turned off. Lack of a Plan B also points to a failure in strategic planning. Rather than assuming successful combat operations will directly lead to the realization of policy objectives, one needs to envision and plan for an end-state that can be realized before operations commence. Furthermore, a successful strategy is also highly contingent on understanding the enemy and having capabilities to implement plans within the context of what is achievable. Here, cultural understanding and knowing what one can or cannot accomplish in given timeframes are critical and should shape the strategy.

Similarly, the German failure to revisit the critical assumption that their Enigma machine messages were secure provided a significant advantage to the allies. Not imagining that their messages were being read, the Germans continued to use Enigma until the end of the war. This experience also points out the role of deception in creating surprise. Both the United States and Britain continually conducted a variety of tactical operations specifically aimed at convincing the Germans that they had no knowledge of Germany's operational plans.

Failure to Adapt to a Changing Situation

Two of the cases assessed in this study highlight the phenomenon of not adapting to the war one finds one's self in, rather than the one that was expected. Little, if any, action was taken to curtail the looting that began after the fall of Baghdad, which was a precursor to the rise of lawlessness and then insurgency throughout Iraq. It took nearly four years for the United States to develop and execute a comprehensive

counterinsurgency strategy in Iraq, largely because of the civilian leadership's insistence to hold on to its original strategy despite growing evidence of an insurgent movement. Additionally, the slow response to IEDs—against the Iraqi populace, the Iraqi security forces, and coalition members—created enormous instability, undercut the perceived viability of the civilian government within Iraq, and threatened public support for the war among the United States and its allies.

Despite the lateness of the counterinsurgency strategy and responses to IEDs, both initiatives have made remarkable contributions to improving the situation on the ground in Iraq. Violence is down and IEDs are more or less isolated events that "we are doing something about." Public support has stabilized and policy erosion has, for the moment, been arrested.

The case of Israel in Lebanon is one in which no solution to the Hezbollah rocket attacks was found throughout the 2006 war. There was no adaptation that solved the problem and this Israeli failure has created—both in the eyes of the Israeli public and the enemies of Israel—a perception that the Israeli Defense Forces are not invincible as once assumed. This view may embolden Israel's adversaries, but it could also lead to more aggressive behavior by Israel to regain the aura of invincibility, which is central to its deterrent capability.

Seams Between and Within Institutions Can Lead to Surprise

The Report of the 9-11 Commission is rife with instances where various governmental agencies did not share intelligence. This is not a new phenomenon, as shown by the attack on Pearl Harbor. Clearly, stovepipes that exist between agencies can lead to the situation where multiple actors know part of the story, but the integration (fusion) necessary for prediction and anticipation that would preclude or mitigate surprise does not occur.

Today's Requirement for Command Knowledge

The limitations of command, control, and communications heighten the potential for operational surprise. U.S. commanders face a growing

challenge to effectively employ an increasingly sophisticated force on an increasingly complex battlefield. Achieving victory requires the commander to orchestrate a complicated mix of assets. This mix includes traditional general purpose forces, "black" capabilities, special operations forces, cyber forces, intelligence sources and analysts, clandestine assets, and interagency assets (*e.g.*, law enforcement, civil reconstruction, homeland security). The existence and characteristics of some of these assets is tightly protected, and the commander has true "command" over some but not all of them. Many assets whose contributions are operationally decisive are often covert and protected by unique security channels.

At the same time, the outcome of operations appears to be becoming increasingly non-linear, favoring those who inflict versus those attempting to counter surprise. The conflicts of the last two decades, in which events shift quickly and unexpectedly, appear to exhibit an increasingly bi-modal distribution of outcomes—either highly favorable or highly unfavorable, with little in between. Put simply, the gradual shifts in conflict have been skewed toward more unexpected, sudden outcomes. As a result, the penalty for ineffective force employment is both more rapid and severe.

Commanders and their staffs face an increasingly severe challenge as they rotate through their jobs. While they are superbly trained in the operations of military forces, they face enormous challenges in understanding the existence, operational significance, technical characteristics, and synergies among the special, covert, clandestine, and interagency assets that might be employed in a given operation. The fact that these critical assets vary by mission area, by region of the world, by changes in threat, and by operational objectives further complicates the challenges.

Operating across multiple security systems both within and across DOD, the intelligence agencies, Department of Energy, and law enforcement agencies adds yet another layer of complexity. In some cases, neither the commander nor his staff have fully acquired the knowledge of how best to employ these capabilities before they are involved in actual operations. In some areas, commanders and staffs start their tours of duty having to unburden themselves from a career's

worth of largely irrelevant doctrine; operational concepts; and tactics, techniques, and procedures—and then master new ones. To achieve this understanding, and to adapt and employ certain assets, requires deep and broad technical knowledge in some cases, but cultural and social knowledge in others. Given the breadth of knowledge required, and the frequency with which commanders and staffs rotate through their jobs, the challenges are daunting.

Finally, DOD has invested heavily to build a command, control, and communications (C3) system for the general purpose force, and multiple C3 systems at various classification levels for intelligence sources. Yet, there exists (at the appropriate security levels) no coherent, operational C3 system across the full range of assets and combatant command, joint task force, and component commands. Similarly, the Department often lacks the command and control tools to adequately understand the "full picture" of U.S./allied, enemy, and neutral assets; truly evaluate alternative courses of action; and plan execution of the preferred courses of action. These all limit the commander's ability to understand the situation and anticipate enemy courses of action. They also expose commanders to unnecessary surprise and similarly limit their ability to inflict surprise on the adversary.

As a result of the Operations Panel's deliberations about capability surprise, there are several steps that the Department could initiate to ameliorate the problem:

- *Re-allocation of classified technology, systems, and operations experts to support the combatant commands, joint task forces, and component units on a continuing basis*. These experts may be drawn from the science and technology, acquisition, war fighting, development, and laboratory communities or from federally funded research and development centers. They should be fully cleared across those U.S. government activities pertinent to the appropriate mission area(s) and threats. This re-allocation should be accomplished no later than the end of calendar year 2010.
- *Re-allocation of C3 and classified program resources and the necessary security policy changes to provide an operational, multi-compartmented network and command and control*

system for the combatant commands, joint task forces, and component units. This network should be assembled in cooperation with the Director of National Intelligence (DNI) (with eventual extensions to the Departments of Homeland Security and State) and adopt a common security policy. The network should permit encryption-based separation of compartmented traffic, and appropriate transmission security protection for organizations and sources whose existence is classified. Most importantly, this network should be equipped with automated gateways and manual transfer points enabling the combatant commands to integrate information across security channels under conditions set by the Secretary of Defense and DNI. Finally, the command and control tools described above should be hosted on this network and engineered to requirements set directly by the combatant commands and those component units designated by the combatant commands. This capability should be established no later than 2012.

Insights for the Future

Historical analysis can provide insights about the future by understanding what others have experienced in analogous situations. Essentially, history can provide vicarious, rather than direct, experience that can be useful in considering options for the future. Nevertheless, although history is not predictive, the cases examined highlight a number of important factors that should be a part of planning for the future:[13]

- The interconnected, globalized world, highly reliant on networked communications and data sharing, provides unprecedented opportunities, but also creates significant vulnerabilities for the United States. Understanding current and future threats, and developing strategies to cope with their potential effects, are necessary steps for protecting key capabilities and for maintaining U.S. capacity to surprise potential adversaries.

13. See also Table 1 for a summary of the case studies, their cause, U.S. response, institutional reaction, and overall lessons.

- Tactical and operational surprises can have strategic effects that far outweigh initial perceptions of their consequences. The Tet Offensive, the Beirut barracks bombing, and IEDs in Iraq all show that policy objectives can be eroded by the reactions of a surprised public to events that, at the time, seem to be either minor setbacks or, in the case of the Tet Offensive, a precursor to an operational victory. The "CNN effect" and the 24-hour news cycle only exacerbate this issue.
- Existing notions for deterrence, largely based on dealing with state actors and framed by Cold War paradigms of massive nuclear retaliation and containment, need to be revisited. These notions, while still useful in some cases, are not universally relevant to current or future security challenges that include asymmetric strategies and non-traditional means of inflicting mass casualties (*e.g.*, biological) or effects (*e.g.*, cyber).
- Small numbers of non-state actors and new capabilities can exert non-linear effects. Here, the examples of Titan Rain, 9-11, and IEDs in Iraq are instructive. In the realms of cyber, biological, nuclear, and even conventional attacks, these actors will certainly become more worrisome and, unlike the paradigm of most state actors, extremely difficult or impossible to deter.
- Future surprises may have a qualitatively different impact than those of the past. In the past, the United States had more robust crisis-oriented civil defense and public health resources that gave it the capacity to absorb attacks, regroup, and respond. There was also more capability to mobilize manpower and industry on a U.S. timeline, because of the nation's physical isolation. This is no longer the case. Homeland security capacities, albeit improved since September 11, 2001, are not sufficient to manage the consequences of surprises from a broad gamut of threats faced by the United States now and in the future. The nation no longer controls the timeline, and usable capabilities will be those that are in being when the surprise happens.
- Because DOD contains much of the U.S. capability to create or respond to surprise, it is a principal target for attack or exploitation. DOD personnel, operations, installations, and

information must be assumed to be at risk from foreign intelligence attack and must act accordingly.

- Strategic deception is clearly an important U.S. capability. Inflicting surprise on adversaries through the nation's own considerable resources is a way to create devastating asymmetries and wicked problems for adversaries. Consequently, strategic deception may be a key to solving wicked problems in the United States.

These general statements can and should be focused on two areas that offer major potential for strategic surprise in the future:

- Current and past U.S. policy still tends to treat space as a neutral area. This simply is no longer the case and thus creates a sanctuary for adversaries. Furthermore, space should be viewed as a potential combat zone and the United States needs policies that will drive both offensive and defensive space capabilities.
- Cyber warfare is happening today. U.S. civilian and military networks are being penetrated every day by sophisticated state and non-state actors. Much like space, the United States has assumed a posture that makes its network-centric society and its national security institutions highly vulnerable to attack and exploitation. The nation needs a strategy that recognizes this reality.

Chapter 1-4. Surprise in the Cyber Domain

Over the past several years, DOD has become increasingly "net-centric." This has entailed deploying network-enabled capabilities and making the necessary changes in doctrine, organization, training, material, leadership and education, personnel, and facilities to execute network-centric operations. A growing body of operational and exercise experience points to the effectiveness of network-centric operations in a variety of situations.

However, for all the increase in capability, DOD's move to net-centricity also brings heightened vulnerabilities—thus creating the potential for surprise. In fact, many have recognized the network as a "center of gravity" for disrupting U.S. military capabilities. The Department's networks are constantly being penetrated today, but these penetrations have not yet reflected the full scope of potential damage that could be inflicted by a skilled, patient adversary.

A central problem is the reality that the knowledge to deliver effective attacks is pervasive. Readily acquired skills to attack, low costs of equipment, and access to networks make the barriers to entry very low. Moreover, since most network defenses are outward looking ("hard and crunchy on the outside, soft and chewy on the inside") insider threats are a serious challenge. Further, the technical, political, and legal complexities associated with attribution and defensive monitoring make deterrence against cyber attack difficult if not impossible to achieve.

In the interest of functionality, rapid acquisition, and cost-reduction, the government (and the commercial systems on which the government depends) is increasingly reliant on commercial-off-the-shelf (COTS) hardware and software. The consistent preference of functionality over security in COTS further increases susceptibilities to attack.

There are several characteristics of cyberspace that create opportunities for exploitation:

- Cyber attacks can be launched remotely, with global effects.
- A cyber attack not only can affect information, but also physically damage equipment and destroy user trust. User trust, once lost, is very difficult and time-consuming to reestablish.
- Attacks on cyber capabilities can be both kinetic and non-kinetic.
- It is difficult, and sometimes impossible, to trace cyber attacks or to attribute them. This characteristic impacts the ability to deter, dissuade, or compel an adversary.
- Cyber-related infrastructure is becoming more and more homogenous (*e.g.*, common operating systems, common routers, and common fibers). This lack of diversity amplifies vulnerabilities because single attacks can have much broader impact.
- Cyber attacks can be conducted autonomously, through "botnets" and similar activities. Like biological agents, cyber attack vehicles can be communicable and self-replicating.
- Counters to cyber attacks often have negative consequences for the defender. For example, disconnecting a user from the network based on abnormal behavior could be equivalent to a self-imposed denial of service attack, particularly if the user is responding to an operational change. Conversely, an active defense mechanism, such as an implant that corrupts or damages a target system, reveals U.S. capability to the adversary. In many cases, these can only be exercised once before the adversary will close that exploitation path to us.

What is Being Done?

There are many ongoing activities aimed at preventing cyber surprise or mitigating the affects should an attack occur. Yet many of these initiatives are in formative stages and reflect only the first steps. Much more will need to be done that builds from these initial steps.

The Comprehensive National Cyber Security Initiative was launched in May 2008. It includes: (1) guidance on departmental assignments, resources, and government processes; (2) strategy for near-, mid-, and leap-ahead initiatives; and (3) initiatives to develop cyber-related policies and to enhance deterrence. This effort is comprehensive in scope. However, it has not yet been adequately funded and its deliverables are not anticipated for some time.

Overall, the department's strategy for meeting cyber challenges is based on a mix of mature and immature approaches. Mature approaches include perimeter defense, enclaves, black cores, key management, and public key infrastructure. Less mature approaches include initiatives in biometrics-based, non-repudiatable identity and identity management, and the trusted computing initiative.

Other initiatives include the following:

- new information assurance policies for the defense industrial base
- steps to increase participation of red teams, and cyber and information operations in exercises and game play
- within the classified domain, development efforts related to war-reserve approaches, hedging strategies and technologies, and ways to sustain trust
- growing interest in the private sector about information assurance
- government partnership with industry to provide more information about threats

Cyber Progress after the Summer Study

Since the conclusion of the summer study activities in late summer 2008, the newly elected Obama administration, at both senior civilian and military levels, has shown a much heightened interest in dealing with the potential for cyber attack. In testimony before Congress, the Pentagon's top information security official cited a 6,000 percent increase over two years in attempts to penetrate DOD networks, from 6 million in 2006 to 360 million in 2008. During the winter and early spring of 2009 the following occurred:

- Upon the President's order, a 60-day review of the U.S. cyberspace posture was completed in May, resulting in a number of key areas for concern. These concerns have been echoed in statements by the President, who has announced the establishment of a new cyber security directorate within the National Security and Homeland Security Staff. In his announcement he said, "It is now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation." He said that we "were not as prepared as we should be" and that we had not invested sufficiently in protecting our digital infrastructure, which he described as a strategic asset.
- The Secretary of Defense announced in June 2009 the creation of a new multi-star multi-service cyber command as a subunit of U.S. Strategic Command. It will be led by the National Security Agency (NSA) director. Among other things, it will coordinate both defensive and offensive activities, something the Defense Science Board has been arguing for over the past several years. NSA likened the need for protection of cyber space to the nearly 200-year-old Monroe Doctrine, which provides declaratory statements about those who would interfere with nations in the Western Hemisphere.
- Senate legislation in April 2009 pushed aggressively to dramatically escalate U.S. defense efforts against cyber attacks, including empowering the government to establish cyber security rules for private networks.
- The Pentagon announced plans to develop a simulated cyber world in which to try out and measure the potential effect of cyber weapons of mass destruction of tomorrow.
- The military service academies are conducting cyber war games as part of their curricula and training. These activities are expected to be extended more aggressively than is current practice to service and joint exercises and war games.

Although these efforts show greater attention being paid to the potential for cyber attack and what to do about it, it is still much too early to determine what the impact and efficacy of this increased attention will be. Hopefully it will push beyond bold statements and bureaucratic actions, but in any case, it is a promising sign.

What Needs to be Done?

Prevention and mitigation are possible, but necessarily involve a wide range of actions aimed at making cyber attacks more difficult and reducing the likelihood of success. Tradeoffs among capability, security, access, and assurance must be made within a risk-management framework since these performance factors typically present competing requirements. The risk management framework should be based on DOD mission priorities and values, but this has never been done well, despite more than a decade of risk management discussions. It is not possible to protect everything all the time. At the same time, risk management in a cyber environment cannot always emphasize security alone. The upside of net-centricity—the ability to conduct operations faster and achieve objectives with fewer casualties—needs to be an integral part of the risk management framework.

Prevention

A key step in preventing surprise is to **understand adversary capabilities and intentions**. The potential "penetrator" must himself be penetrated, and not solely by cyber means. All disciplines of intelligence, especially human intelligence and signals intelligence, must be brought to bear and then correlated to understand present and future threats in cyberspace.

Ideally, a cyber attack can be deterred before it even begins. A variety of games and studies suggest it is very hard to compel or even persuade an adversary to give up information-gathering activities in cyberspace once they have begun—the combination of clear attribution and coercive tools to increase the cost above the gain is not often possible in this domain. Similarly, since barriers to entry are so low and the potential utility so high, it is hard to dissuade a nation or non-state actor from acquiring cyber capabilities. Thus, deterrence of unwanted behavior in cyberspace has become the focus of several intense reviews. The emphasis is not to try to deter cyber attacks solely through cyber means, but to combine the full instruments of national power—military, information, diplomatic, legal, intelligence, financial, and economic—to bring pressure or impose costs or doubts on an adversary.

The U.S. military's shift to become more "net-centric" is providing significant operational and tactical advantages in many different environments. However, this brings with it increased dependence on the network and its data and, therefore, increased vulnerability. Adversaries understand this, and the Department's networks, people, and processes are under almost constant pressure. Yet, too many leaders still treat the network as a technical capability that primarily is the province of the "techies." Worse yet, some consider it as an administrative support mechanism that should be transparent to users. On one level, this is true—users should not have to be experts in the high-tech processes of installing patches or reconfiguring hardware. But there is a more central issue tied to the use of the network in leveraging war fighting capabilities.

Fundamentally, the network has become a combat capability, and it needs to be treated with the same attention as other major weapon systems.[14] As network-enabled capabilities are deployed, changes need to be co-evolved across the full range of doctrine, organization, training, material, leadership, personnel, and facilities (DOTMLPF) to execute network-centric operations. The network needs to be operated securely and defended when under attack, and the information on the network needs to be managed effectively. This issue is not simply a technical one. The people, processes, and technologies need to be resourced sufficiently to outpace a rapidly evolving threat. Moreover, given the interdependence of networks and the functions of national security, a "whole of government" effort is needed, as well as partnership with the private sector. The Critical National Cybersecurity Initiative has begun to address these issues, but in fact it really only has just begun. It is essential that the initiative be sustained and resourced so that capabilities and products are actually delivered.

The provenance of hardware and software needs to be addressed throughout the product life cycle. DOD systems depend heavily on globalized COTS components. Too often, security activities focus on the operational phases of a product's life, but the globalized supply chain demands that security be addressed at each step from

14. *Defense Science Board 2006 Summer Study on Information Management for Net-centric Operations, Volume I: Main Report* (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics: Washington D.C.) April 2007.

concept development through end-of-life disposal. Since both processes and personnel can introduce vulnerabilities that may stay dormant for extended periods, both need to be examined. For example, the complexity of hardware and software products hides both intentional and unintentional vulnerabilities. Critical system components need special attention from a security point of view, and personnel vetting should extend to people who provide the capabilities, as well as those who operate and oversee them.

Information technology operations need to be assured through a comprehensive approach at several levels:

- The characteristics of the services to be delivered must be specified. Commercial service level agreements (SLAs) provide a basis, but DOD tends not to observe the conditions of SLAs. Often DOD chooses frugality over needed performance and security until the system breaks.
- Assurances are needed with regard to people. These often aren't addressed in SLAs related to information technology operations. For example, DOD at one point engaged with a WebEx service [Internet-enabled conferencing and collaboration] that was partly operated in and through China.
- Operational networks depend on every operator being trustworthy. Once on the inside, there are few checks and balances. This is not realistic, and poses exceptional risks in the case of malicious activity by cleared insiders, or by outsiders who have succeeded in getting a presence on the network. Not only do sensors need to monitor activities on the network in near-real-time, but means need to be in place to detect anomalous behaviors, recognizing that this is very hard against a skilled, patient adversary. In some cases, solutions like two-person integrity need to be implemented, with "no-lone zones" at critical nodes.
- Non-DOD-specific contract vehicles or "masked" acquisition channels provide one level of protection from attempts to target our supply chain. For example, targeting a blanket DOD personal computer (PC) acquisition vehicle and its associated production line could provide a lucrative, and reasonably-sized,

target for adversaries. Expanding the procurement of PCs for the Department to a larger number of commercial suppliers, without identifying specific DOD ties, makes the target environment much broader and, therefore, much harder to exploit.

- Help desk information can provide insights to adversaries. For example, a raft of calls to a router supplier help desk with escalating priorities from a specific individual, set of individuals, or government organization representative would likely indicate an outage or problem affecting an important operational capability. This could be exploited in at least two ways. One is by indicating a loss of U.S. operational capability that could be exploited opportunistically to support an adversary operation. The second is to provide indications that an exploitation perpetrated by an adversary has been successful. Interestingly, simply knowing that the calls have been made from a location over some period of time may be sufficient to alert an adversary; the content of the calls need not be known. In order to prevent these kinds of exploitations, help desk support to DOD entities should remain in the United States, protected (to the extent possible), and manned with vetted personnel.

The network also has to be defended on several levels. The foundational step is to characterize and manage "normal" operations. Network mapping and discovery should be a routine part of network operations activities. Tools should be available and used routinely to provide resources as a function of demand.

Defenders must be knowledgeable about current tradecraft. Classification related to cyber issues has made this harder than it needs to be. Many technical or social engineering techniques that are considered classified by the government are well known in the hacker community.

Strong authentication and identification are essential. The role of biometrics needs to be considered carefully, including downsides like unchangeable characteristics. The ability to drive out anonymity would aid significantly in establishing dynamic communities of trust in response to operational needs. This, however, is a double-edged sword,

since it complicates operations and makes it more difficult to gain access on those missions that require anonymity.

Cyber capabilities need to be more robust and enhancements need to proceed along several parallel paths:

- Capacity should be provided beyond expected needs. Networks are often unprepared for surges or future requirements. Excess capacity is an underlying tenet of successful network protection efforts in the commercial world.
- Diversity should be built into the networks, support equipment, and operating systems. Heterogeneous approaches make it harder for the attacker and provide opportunities for graceful degradation. Diversity also provides some buffer against the cascading effects caused when complex, adaptive systems that are too tightly coupled begin to fail.
- The ability to rapidly reconfigure the network and reconstitute capabilities under stress should be part of the network design and operations strategy.
- The network should have classified war reserve modes, with a control channel that's "out of band" from the normal network (see last bullet below).
- Critical subsystems and applications should have higher levels of assurance, with robust designs that incorporate "trusted" electronics.
- The network should be able to operate in degraded modes, with protected "high security" islands.
- Functionality needs to be balanced with security. COTS products, in particular, may provide more functionality than government users need, but offer inadequate levels of security against a determined opponent. Configuration control is important. At the same time, care needs to be taken not to impose so much security that the mission cannot be accomplished, or that workers are driven to develop "workarounds."
- There should be a separate network for information assurance battle management, reconstitution, authentication key

management, out-of-band signaling, and service level agreements with enforceable definitions. This also could serve as the control channel for war reserve modes.

The U.S. derives significant advantage from having world-class cyber assets and capabilities in the country, and these should be maintained. These U.S. advantages apply in two broad areas: physical assets and intellectual capital.

Having Internet service providers (ISPs), switches, connectivity, and databases on U.S. soil provides clear lines of enforceable legal authority and responsibility across a spectrum of activities. It also provides opportunities for support to law enforcement and intelligence. Some 80 percent of global communications traffic currently runs through U.S. nodes, but some of this traffic, and the key nodes, are beginning to move offshore. Thus, government policies and practices should encourage the continued operation of key communications and computing nodes inside the country.

Equally important is U.S. market leadership in cyber-related products and services, and research and innovation in the information technology sector. Research should be focused on high-leverage solutions such as identity management, encryption, deep packet inspection, and tagged security architectures. The U.S. should actively influence next generation computer and internet design. A growing concern is the lack of basic research investment in this and other sectors—the nation is still living off the fruits of research from the 1970s and 1980s.

DOD itself—indeed government in general—must recruit, train, and retain a skilled cyber workforce. Modeling and simulation can be leveraged, and closed networks are emerging on which much better training can be done. Cyber tactical and operational skills will become as, or more, valuable in future warfare as more conventional specialties are today.

Mitigating Cyber Surprise

Cyber attacks are hard to detect and to characterize, but detection and characterization must become a fundamental capability if cyber surprise is to be mitigated. Actually, the word “attack” is very often over-used. The

Joint Task Force, Global Network Operations, recognizes different categories of cyber incidents, ranging from probes to activities that gain root access. Although DOD computers are continuously probed, and sometimes exploited or compromised, it is hard to distinguish between a "crime" and an "attack," even if anomalous events are detected. Steps need to be taken in three broad areas:

1. Collection and exploitation of operational data
2. Distinguishing anomalous behavior of systems, equipment and people
3. Strengthening tools for attribution, including both technical and legal tools for trace back, and developing an ability to follow both social and technical trails

Other mitigation steps involve **preparing for degradation** along the dimensions of availability, integrity, confidentiality, authentications and identity, and trust. For example:

- Does my information technology have the capacity to support the mission? (availability)
- Are my data correct? (integrity)
- Are my secrets safe? (confidentiality)
- How far can/should I trust the identities of teammates I can't see and/or don't know? (authentication)
- How confident am I in the answers to these questions? (trust)

Plans and exercises should incorporate realistic degrees of degradation in each of these dimensions to understand how to live with less than perfect answers to all the questions above, to figure out how these dimensions interact with each other, and to learn how to restore trust when it is lost.

Capturing forensics information for attribution and distinguishing anomalous behavior is a key to viable mitigation and recovery strategies. Once an attack has been detected, a commander must be able to reconfigure and reallocate resources to continue the mission. Several key steps that should be taken include:

- Taking advantage of emerging technologies designed specifically for resilience, such as *ad hoc* networking and peer-to-peer. Many of these introduce new security issues that must be balanced with their advantages, but they need to be considered. The emerging project at National Defense University known as "Social Software for Security" (S3) seeks to facilitate government use of these approaches, taking a clear-eyed view of both their opportunities and challenges.
- Coordination with theater and combatant commanders. Actions to mitigate risk, such as imposing "minimize" on communications to limit users and reduce traffic, provide significant benefits for operations.
- Architecting the network such that sessions can be prioritized and delivery of critical information is guaranteed. This requirement is facilitated if the network has been provisioned with excess capacity as recommended above.

Overall, the goal of mitigation measures should be to achieve "mission assurance," vice "information assurance." In other words, the commander must be assured of continuous operations under all levels of attack. Capabilities should degrade gracefully. A prerequisite is to understand the behavior of the network under various levels of degraded conditions—an area that needs significant research. Users need to be able to move up and down among network classification levels during periods of degradation.

Managing Cyber Surprise

Figure 1-1 offers a framework for handling cyber surprise in the context of strategy, plans, and preparations. It also provides an assessment of current readiness. Three cases are addressed:

1. prevent surprise (influence, uncover, eliminate)
2. deal with surprise (stabilize, mitigate, recover)
3. create surprise (adapt, reverse, reshape)

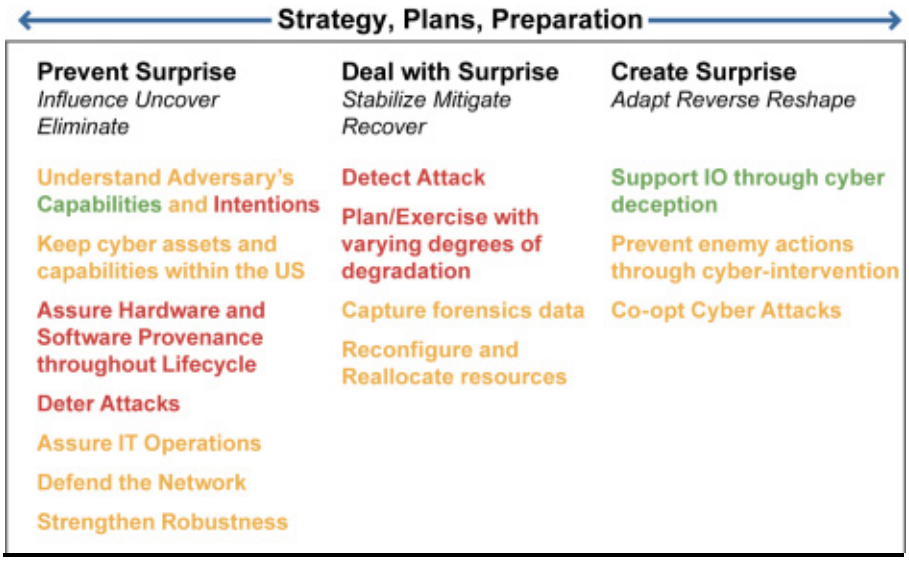


Figure 1-1. Managing Cyber Surprise

Of the 16 capabilities examined during this study, two were considered "green" (satisfactory), five were "red" (unsatisfactory), and the rest "yellow" (not ready, but some progress being made). "Green" areas included understanding an adversary's capabilities and supporting information operations through cyber deception. The five "red" areas are: understanding an adversary's intentions, enforcing needed hardware and software provenance, deterring attacks, detecting attacks, and planning and exercising with varying degrees of degradation.

The remaining areas, judged "yellow," are:

- encouraging the [continued] operation of key communications and computing nodes in the United States
- maintaining U.S. leadership in information technology
- assuring information technology operations
- defending the network
- strengthening robustness
- capturing forensic information
- reconfiguring and reallocating resources
- preventing enemy actions through cyber-intervention
- co-opting cyber attacks

What Prevents Us from Taking Action?

The question remains: If we understand the criticality of the nation's information infrastructure and know some of the necessary preventative and mitigating measures, why aren't adequate steps being taken? The bottom line is that preventing and mitigating cyber attacks is difficult and expensive and cuts across every individual entity within the DOD as well as virtually every other governmental agency. But other factors play a role as well—many related to risk mitigation tradeoffs. The principle factors among them are discussed in this section.

Reducing vulnerability to cyber attack is really hard and likely expensive. The overarching reason behind the nation's continued vulnerability in cyber is the deeply complex nature of its constituent hardware and software—a complexity that stretches the bounds of human understanding and is unlikely to be fully understood for decades to come, if ever. Indeed, its complexity continues to increase at an exponential pace. An attacker has an almost infinite range of possibilities within this vast domain to attack remotely or from within a system itself, or to insert malicious code or hardware modifications. The defender has little chance of finding hardware or software modifications or detecting an attack, and even greater difficulty in attributing the activity. In short, this is a really, really hard problem and even moderately effective preventive measures are likely to be quite expensive. It would be easy to conclude that nothing can be done and save the effort and money—though we assert that that is not the right conclusion.

The perception is that the nation has not been badly hurt, yet. In the face of this great complexity and expense, there is the perception and rationalization that the nation has not yet been badly hurt by a cyber attack. In spite of the continuing rain of low-level hacker intrusion attempts against all military and commercial systems, many administrators believe that these systems have never been breached or that they have never suffered serious damage. Over time, administrators become increasingly confident of the invulnerability of their systems and become somewhat complacent. However, this confidence is unwarranted. Given the difficulty of detecting attacks, they might not realize or appreciate their vulnerabilities. Moreover, these low-level attacks, usually

from hackers, do not reveal the vastly greater capabilities in the cyber arsenals of nation-state adversaries or well-organized non-state actors.

There are no objective measures of success, and the final reckoning comes only at wartime. How does the nation know how well it is doing at defending against cyber attacks? Unfortunately, today there are no objective metrics to quantify progress or to do cost/benefit analysis, although we argue that such metrics should be developed to whatever extent possible. Absent these metrics, the reckoning comes in wartime, when the adversary employs the tools and techniques reserved for such contingencies. Only then might it be possible to discover the true effectiveness or ineffectiveness of U.S. defensive measures.

There is no means to differentiate between what is strategic and what is merely important. The difficulty in prioritizing threats is a pervasive conundrum. We as a nation are convinced that cyber poses a critical strategic threat—indeed some believe that it is the only "known surprise" that has the potential of completely disabling U.S. military capability. Yet, cyber is only one of many potential threats clamoring for funding and support, and even within the cyber environment itself there are myriad approaches competing for limited resources. Until very recently, no serious integration and coordination of cyber effort existed. Therefore, it is particularly difficult in cyber, where the nation has not yet experienced expert attacks from nation-states, to apportion and prioritize resources and approaches.

We don't learn well from government or commercial experience. The stove-piped organizations that largely exist today inhibit information sharing within government. There is also much to be learned from commercial industry, where there is considerable experience in defending attractive financial targets. Unfortunately, much of this experience is kept secret in order to prevent embarrassment, inform competitors, or empower attackers.

Defense is not often well-informed by the offense. Many system architects and administrators are unaware of the true capabilities of expert attackers. Although the government employs many such experts in offensive cyber warfare, classification, some legal issues, and organizational barriers often prevent this expertise from being shared with defenders.

Industry sometimes has no business case for increased information assurance. Absent regulation, industry only implements capabilities for which there is a strong business case. For example, a switching center might constitute a point of vulnerability in a commercial network being used by DOD. But the construction of a geographically-diverse backup center would be expensive and would not bring in commensurate revenue to the carrier. Thus, the carrier would not be incentivized to construct such a center, in spite of its potentially vital role in providing information assurance.

The majority of the political leadership does not understand the cyber problem or domain. Ultimately, the purse strings are controlled by the political leadership. Although many are computer literate, deep understanding or appreciation for both the criticality and vulnerability of the country's cyber capability is largely absent, and thus prevention and mitigation become secondary to other more visible and understandable threats.

We as a nation consistently emphasize what we know how to do, rather than balancing all attributes. There is an old and oft-repeated saying, that to a hammer all the world looks like a nail. In the cyber domain, the hammer is often seen as encryption for confidentiality. Thus, there is an assumption that if data are encrypted, the network is secure. Unfortunately, this is far from true.

Steps towards an international control regime would expose a "say-do" gap. The problem of defending the U.S. cyber infrastructure is so deeply complex that, in spite of the great difficulties in effecting deterrence, it must be seriously considered. One approach to deterrence, mentioned previously, is to encourage an international control regime. However, this would expose the nation's own offensive program to scrutiny.

Conclusions and Recommendations

The Operations Panel of this study has several recommendations that will improve the nation's cyber posture.

RECOMMENDATIONS: CYBER SURPRISE

Chairman, Joint Chiefs of Staff, direct a series of exercise activities to improve operational understanding of the criticality of information systems to warfare. These should include:

- Conducting regular exercises under degraded conditions, with the conditions of degradation being iterated and made more severe from year-to-year.
- Promulgating tactics, techniques, and procedures and rules of engagement to assure mission success under degraded cyber conditions.
- Developing and implementing approaches to re-establish trust after network degradation.
- Providing definitions of the necessary and affordable characteristics of network service levels, and under what conditions and for which missions.
- Establishing objective measures of success for all information technology mission capabilities to inform architecture and engineering decisions (availability, utilization, and scalability)

DOD direct a series of activities to increase adversary resistance of critical information systems (and other critical infrastructures that depend on information systems) through a series of activities. Such steps should include:

- Strengthening deterrence through improved detection and attribution methodologies.
- Increasing the competence and trustworthiness of the cyber workforce.
- Directing consideration of provenance within a global supply chain for the acquisition of all hardware and software.

- Evolving towards pervasive, strong authentication and identification capabilities.
- Building a separate network for information assurance battle management, reconstitution, authentication key management and out-of-band signaling.

Chapter 1-5. "Surprise" in Space

Space is another area in which "known" surprises may arise. The use of space has become increasingly important to the United States and many of its peacetime and wartime capabilities depend on accessibility to space. Thus, denial of that accessibility presents an opportunity to the nation's adversaries, introducing vulnerabilities that can lead to surprise. The importance of space is well documented in policy. On August 31, 2006, the President signed a new National Space Policy initiative, which highlights the importance of space to the nation and presents goals for our country's space activities. This policy has been relatively constant since 1996, and in principle, for decades.

One key assumption underlying this policy is that the nation can ensure the continued availability of several key capabilities, including strategic and tactical communications; missile warning; and position, navigation, and timing (PNT). It is also critical to assure the proper integration of systems across the national security space domain, as well as with air, land, sea, and cyberspace, and to ensure the viability and proficiency of the nation's space professionals.

U.S. Dependence on Space

The United States relies on space capabilities not only to meet the needs of joint military operations worldwide (Figure 1-2), but to support the nation's diplomatic, information, and commercial efforts as well. Because of this, it is important that national security space operations and space professionals are integrated into all aspects of peacetime and wartime operations—providing robust and responsive space capabilities around the globe.

Commercial communications satellites are providing direct support to war fighting forces. Recent data indicate that over 80 percent of the satellite communications used in U.S. Central Command's area of responsibility is provided by commercial vendors.

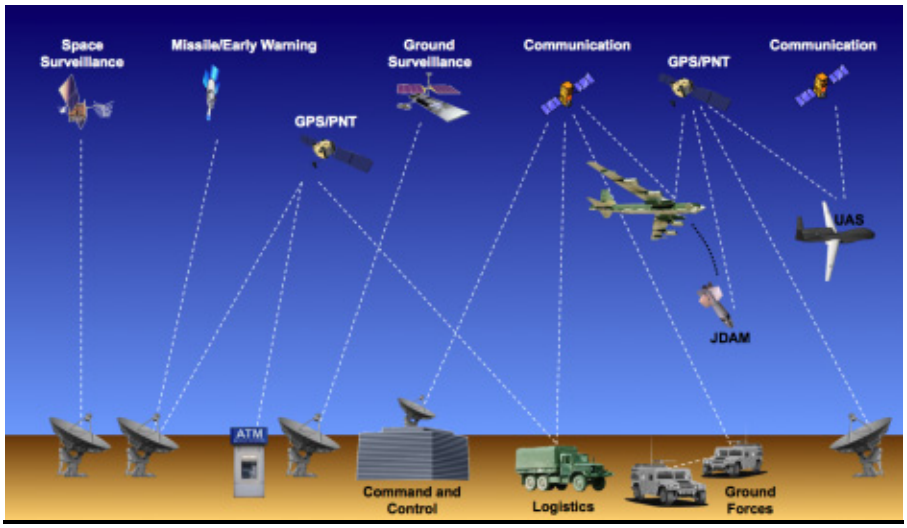


Figure 1-2. Importance of Space in the 21st Century

U.S. public and commercial sectors also rely on the access and use of space capabilities in many areas of everyday life. From banks and financial institutions employing global positioning system (GPS) timing to synchronize their encrypted computer networks to forecasting severe weather, America is increasingly dependent on capabilities from space. The space community continues to provide continuity of service in key areas, while simultaneously working to modernize and recapitalize the aging space fleet and infrastructure to address the future space environment.

Globally, the rate of change of technology in the 21st century and the number of nations directly engaged in space continues to increase. The capacity to contest space operations and capabilities is also growing. Space can no longer be considered a "safe haven" or "sanctuary." Recent Chinese testing of a kinetic anti-satellite weapon demonstrated an ability to challenge, disrupt, or destroy space assets and capabilities. This test also raised global concerns over space debris and the debris' potential to collide with space assets in, or traversing through, low earth orbit. Thus, space situational awareness (SSA) has become increasingly important to provide the visibility needed for a better understanding of activity in space. The nation must continue to work to protect its space capabilities in a potentially hostile environment.

Other surprises have occurred in space. Besides the China test on January 11, 2007, with a missile kinetic kill of one of its own spent weather satellites, Libya successfully jammed communications satellites in the 1990s. And as far back as the early 1960s, there were satellite failures related to Project Starfish that produced radiation enhancement of the Van Allen belt. The United States created a recent surprise of its own in 2008, with the successful destruction of a National Reconnaissance Organization satellite with a Navy Standard Missile-3 (SM-3) interceptor.

What is Being Done?

Many prevention and mitigation activities related to U.S. space capabilities are ongoing today; some are described below.[15] Among the most prominent are the following:

- A Space Situational Awareness Roadmap has been submitted to Congress.
- A Space Protection Strategy has been developed.
- Initial efforts at addressing continuity of service for strategic communications; missile warning; and position, navigation, and timing are underway.
- The Operationally Responsive Space Office was established in May 2007.

Integration

Integration and collaboration across the national security space community—across functional areas such as ISR and across organizations within DOD, other government agencies, industry, academia, and Congress—is extremely important. Integrating architectures and protection of space assets are also become increasingly important as systems become more capable of dynamic tasking and mutual cueing.

Several forums and dedicated organizations are in place to help. The Space Partnership Council, with membership from organizations across

15. Related published reports include an Operationally Responsive Space Progress Report to Congress (Summer 2008).

the national security and civil space communities, is helping to share best practices, avoid duplication, and support integration of space activities. The U.S. Strategic Command has established the Joint Functional Component Command for Space (JFCC SPACE), headed by the Fourteenth Air Force Commander at Vandenberg Air Force Base. This action provides a single commander, with a global perspective, enhancing functional integration for the command and control of the nation's space-based assets.

Launch

The United States recently accomplished its 58th consecutive, successful national security space operational launch—a national record. A continuing commitment to mission assurance and exacting attention to detail is necessary to help enable assured access to space.

Missile Warning

Space-based infrared sensing capability (*e.g.*, missile warning, missile defense, technical intelligence, and battlespace characterization) remains a critical requirement. In addition to the current Space-Based Infrared System (SBIRS)-High program, work should begin on the next generation of infrared surveillance systems. It is important to develop a range of options to ensure that the nation's missile warning capability is both sustainable and responsive. For example, developing options based on wide field-of-view focal plane arrays for the "SBIRS-type" missions could potentially be fielded on smaller satellites to provide a more responsive capability.

Each operational capability area, such as missile warning, should have an investment strategy and portfolio that goes beyond the current program of record, to include needed work to support successive generations of improved technical capability for space and ground elements alike, as well as for end-user equipment.

Communications

Both continuity of service for strategic communications and management of an ever-increasing demand for high bandwidth capacity are

essential. The Advanced Extremely High Frequency (AEHF) program, the follow-on to the Military Strategic and Tactical Relay (MILSTAR) program, successfully completed its first end-to-end communication test with legacy MILSTAR terminals in June 2006, and is scheduled for first launch in 2010. The Wideband Global SATCOM (WGS) system has begun to provide high capacity communications in the X-band and the KA-band frequency range. The first WGS satellite, launched in October 2007, is on orbit and operational. The second (of six total satellites), WSG-2, was launched in April 2009 and WSG-3 was launched in December 2009. Australia has entered into a partnership with the United States to receive high bandwidth capability from WGS and has provided key funding for the WGS system. Participation of U.S. allies in cooperative space programs should become increasingly important.

Position, Navigation, and Timing

Continuity of position, navigation, and timing capability is critical for military, civil, and commercial applications, and GPS is the world's standard for space-based PNT. Using GPS, military and civilian users can access highly accurate, real-time, all-weather, position, navigation, and timing data 24 hours a day, 7 days a week. Assured GPS capability is crucial to the success of many missions, from humanitarian relief to weapons employment, and the Air Force is committed to continuity of this critical service. To that end, the United States should continue to make improvements to the constellation—including new civil signals, more jam-resistant military code, new receivers, and increased accuracy. In 2006, interagency coordination was strengthened through an active National PNT Executive Committee, co-chaired by the Deputy Secretaries of Defense and Transportation, and the stand-up of the National PNT Coordinating Office.

PNT needs for the war fighter are being addressed through increased power and signal improvements to eight GPS IIR-M satellites (three on orbit and five awaiting launch), twelve GPS IIF satellites, their ground control systems, and associated user equipment. Together these actions will deliver higher power and improved anti-jam capability.

Anticipating future needs, the Joint Requirements Oversight Council validated the GPS III requirements to include increased power beyond

GPS IIF, an L1C signal, enhanced cross-links, and spot beam capability. These capabilities will enhance current GPS capability, and are planned to be delivered incrementally, or in "blocks." The first block, GPS IIIA, will incorporate GPS IIF capabilities plus a tenfold increase in signal power, a new L1C civil signal compatible with Galileo [a global navigation satellite system], and a growth path to future blocks. GPS IIIB will then incorporate enhanced cross-links capability, and GPS IIIC will provide spot beam capability.

Space Situational Awareness

Space situational awareness is the foundation for space protection strategy and includes systems such as the Rapid Attack Identification Detection and Reporting System (RAIDRS) program, the Space Fence, and the Space-Based Surveillance System (SBSS).

RAIDRS develops ground-based systems that rapidly detect, locate, characterize, identify, and report interference with DOD-owned and DOD-used space assets, and it is being developed via a block approach. The initial capabilities should be able to detect and geo-locate satellite communications interference via fixed and mobile ground systems, with follow-on blocks planned to provide automated data access/analysis, data fusion, and decision support capabilities.

The Space Fence is planned to replace the aging Air Force Space Surveillance System (AFSSS) with a system of three sites worldwide and will use a higher radio frequency to detect and track smaller-sized space objects. It would expand the terrestrial-based detection and tracking capability, supporting space situational awareness while working in concert with other network sensors.

Building on the Space-Based Visible (SBV) technology demonstration, the SBSS program is planned to deliver optical sensing satellites to search, detect, and track objects in earth orbit, particularly those in geosynchronous orbit. Surveillance from space will augment ground sensors with 24-hour, all-weather search capability. SBSS is planned to be fielded as a pathfinder capability to replace the aging SBV sensor and, as a follow-on block of surveillance satellites, is then scheduled to provide increased worldwide space surveillance.

To address the rapidly evolving space environment, acceleration of these programs and development of needed, additional future capabilities are warranted.

Efficient Acquisition

The space acquisition approach should continue to emphasize integration and collaboration among interested parties in all stages of the acquisition process. A goal is to create partnerships within the space community which are critical to this community's success. The military should provide well-coordinated requirements, vetted through operators, acquirers, and logisticians. The government acquisition community, working with industry, must assure that technology is mature and that systems engineering and manufacturing capabilities are in place to deliver systems that meet requirements—on cost and on schedule—with appropriate funding stability.

The "Back to Basics" initiative remains a key construct to improve space acquisition. This initiative promotes a renewed emphasis on increased discipline in the development and stabilization of requirements and resources, engineering practices, and management, as well as a more deliberate acquisition planning strategy. A goal of funding to a cost estimate at the 80 percent confidence level also helps ensure successful space acquisition program execution. For most space systems, a "block approach" acquisition strategy that is focused on delivering capability through discrete, value-added increments is encouraged. Programs with defined, executable block strategies should reduce production risk, deliver incremental capabilities to the war fighter sooner, maintain continuity of service, and enable resources to be applied—thus providing additional capability options consistent with the 21st century space environment.

Operationally Responsive Space

In 2006, the Air Force established the new Space Development and Test Wing, headquartered at Kirtland Air Force Base, New Mexico, located next to the Air Force Research Laboratory's Space Vehicles Directorate. The organization focuses on the development and testing of smaller satellites/orbital assets, with the goal of increasing innovation

and speed, to rapidly transition ideas to fielded capabilities. A joint Operationally Responsive Space (ORS) office was stood up in May 2007 nearby to support coordination and integration across the national security space community. The ORS efforts include developing the ability to launch, activate, and employ low-cost, militarily useful satellites that can provide surge capability, reconstitute or augment existing constellations, or provide timely availability of tailored or new capabilities. The ORS construct should support an increased ability to transition rapidly from experiment to operational capability.

A broader view of ORS is a tiered capability consisting of spacecraft, launch vehicles, and ground segment to deliver a range of space effects to the war fighter. Additionally, this broader view combines existing, ready-to-field, and emergent systems that are focused on reducing development and deployment costs and schedule.

The first on-orbit experimental tactical satellite, TacSat-2, was successfully launched in December 2006, with the launch of TacSat-3 following in May 2009. The TacSat-2 satellite was developed quickly and cost effectively, carrying several experiments to test cutting-edge capabilities to support the war fighter. The TacSat-2 team demonstrated "responsive" capabilities by efficiently integrating the satellite and launching on a Minotaur booster (Minuteman derivative) within seven months of ordering the booster.

What Needs to be Done?

Although the previous section describes a number of recently initiated or planned activities to strengthen the resiliency and surety of U.S. use of space, most of these activities have either yet to produce an actual capability or have not proceeded very far beyond the planning stage. Moreover, they are not yet well integrated, nor are they funded at a level to ensure robust defense and/or reconstitution of assets in space.

The study members believe that a greater sense of urgency should be placed on these activities, as well as on others outlined below but not yet initiated. U.S. dependence on space, the existence of serious vulnerabilities, and the widespread knowledge and capabilities to challenge the nation's use of space all conspire to make this a very

serious problem. The potential denial of some critical space capability should not come as a surprise, yet if the United States fails to act decisively, it no doubt will.

Implementation of the Space Situational Awareness Roadmap (excepts from the roadmap's executive summary are provided in Appendix 1-A) would be an important basic step toward reducing uncertainty and informing operational investment options to help prevent or mitigate surprise in space. But there are many other steps that should be pursued as well—actions that build from the current activities and that must be implemented with the sense of urgency described above.

- Implement a converged/unified view for a more robust national security space architecture.
- Accelerate improvement to space situation awareness, including surface-based, space-based, and common operating picture capabilities.
- Regularly include degraded space environments in war games and exercises. In some cases, exercise to the point of breakage, so that military forces can learn what true vulnerabilities exist and how to work around them. Use the combination of exercising and red teaming to inform each other.
- Develop options for robust launch capability.
- Establish a coordinated effort in the Department of Defense to reduce mission-critical reliance on space capabilities by providing some ground-, sea-, and air-based alternative workarounds.

Space Professionals/Workforce

Another area where a great deal of attention is needed is in maintaining and building a cadre of space professionals in the military, civil service, and industry, as these individuals serve as the foundation for future space capability. Some of the most space-experienced personnel will soon be eligible to retire, so it is critical to attract and retain technically skilled people to maintain the technical foundation and essential skill sets required to accomplish the nation's space

missions. Better cross-functional assignment practices to more effectively match individual competencies and experiences with position requirements are also important.

The importance of space as a force multiplier underscores the criticality of a strong industrial base that will be able to satisfy military requirements, both now and in the future. The Space Industrial Base Council is a forum to address space industry issues and bring together stakeholders from across government to provide coordinated attention and action on space industrial base issues.

The space cadre must be comprised of the most highly qualified personnel possible. The National Security Space Institute (NSSI) continues to be a DOD center of excellence for space education and serves a diverse multiservice and governmental agency population. Additionally, the NSSI, Air Force Institute of Technology, Naval Postgraduate School, and other academic organizations continue to develop new distance learning courses, making coursework available to a larger audience, and allowing students to work and study simultaneously.

The significance of having a high-quality workforce will only grow as the global development of space expands. Just as the block approach provides a path for the development and maturity of technology, it also provides the opportunity to develop future space leaders through experience gained with increasingly complex systems. Hands-on experience in building, launching, and operating spacecraft through ORS and small satellite programs help develop technical instincts and the experience base for effective program management in the future.

The National Defense Education Program provides additional opportunities for scholarships in math, science, engineering, and foreign language, with a focus on critical skills for clearable people. The defense laboratories and product centers help sponsor the students and provide mentorship for the next generation space leaders.

Conclusions and Recommendations

The United States critically depends on its space capabilities as an integral part of military power, industrial capability, and economic vitality. Our nation must continue to ensure continuity of services in

critical areas such as missile warning; strategic and tactical communications; and position, navigation, and timing. The members of this study recommend a strong and urgent focus on strengthening and integrating America's space efforts, which include the following specific recommendations.

RECOMMENDATIONS: SPACE SURPRISE

- DOD/U.S. Strategic Command formally state requirements for a more robust space architecture (high/low mix):
  - Pursue improvements in space situational awareness—surface, space-based, and an automated space common operating picture
  - Require rapid space reconstitution and augmentation capabilities
  - Require non-space backups for missile warning, strategic communications, and precision navigation and timing capabilities (*e.g.*, augmentation via high-altitude, long endurance (HALE) systems and better weapon system inertial measurement units (IMUs))
- Joint Forces Command incorporate realistic space degraded environments into joint/combined war games and virtual, constructive, and live exercises. Iterate lessons learned with ongoing Service and combatant command red team and with the Office of the Secretary of Defense (OSD), Office of Net Assessment activities.
- Based on the above, learn how, practice, formalize, and adapt measures to fight through degraded space environments.

U.S. Strategic Command should take the lead in stating formal requirements and vet those requirements through the Joint Capabilities Integration and Development System (JCIDS) process. Representatives from all affected government departments need to be involved in drafting the requirements; however, the requirements should be formalized within the DOD process.

Chapter 1-6. Preparing for Operational Surprise

The spread of technology (Internet, I-Phone, etc.) and the emergence of non-state actors on the strategic level (Al Qaeda) offer more opportunities for operational surprise. However, without specialized training, the typical operational commander will have difficulty responding effectively to operational surprise, let alone creating it.

Creating Surprise

Creating operational surprise is highly prized, very difficult to orchestrate, but, nonetheless, a critical discipline and technique to develop—both at the operational and strategic levels. A key ingredient embedded within operational surprise is the age old practice of deception. Deception can magnify strength for both attacker and defender, and is among the least expensive military activities in terms of forces and assets. Surprise is easiest to create when the surpriser reinforces what the adversary thinks and, then, acts contrary to it. Perhaps the most successful strategic use of military surprise/deception was Allied Plan Bodyguard—adopted in January 1944 to mislead Hitler and the German Supreme Command about the place and time of the allied invasion of France.

Creating strategic surprise is especially challenging. Indeed, creating operational and strategic surprise requires one to undertake a sequence of sophisticated, orchestrated events, all of which the adversary must believe, while protecting one's own assets (*e.g*. double agents). In order to undertake such an endeavor, one must have a sophisticated understanding of the adversary's intelligence-gathering processes and political/decision cycle—as well as the soundness of its operational and tactical doctrine. Even with this information, plans that rely primarily on deception or bluffing often fail.

Thus, this study concludes that creating strategic and operational surprise will remain key ingredients for success on both the battlefield and the political front. As a result, we recommend that the Secretary of

Defense create a capability for developing strategic surprise. Specifically we recommend that the Secretary task both the Under Secretaries of Defense for Policy and Intelligence, and the Joint Staff, working with the Office of the Director of National Intelligence, to create a tiger team to lay out courses of action and a way ahead for establishing a standing strategic surprise/deception entity. Once the initial work has been completed, all parts of the interagency should be brought into this effort.

Yet this is but one component of the central recommendation that emerged from the deliberations of this panel, namely that the United States needs to elevate its capacity both to create and to cope with strategic surprise. To do so requires marked improvements of existing capabilities, principally in the realm of preparation, rather than execution.

It is our belief that the United States military is without peer in its ability to visit surprise on adversaries at the tactical and operational levels. Technology-enabled capabilities—such as stealth, network-centric operations, precision strike, and a host of others—in the hands of highly trained and competent forces provide the United States with a capability that is both envied and feared by friends and adversaries. U.S. military forces also have the inherent capacity to respond to tactical and operational surprise. They are resilient, adaptable, and steadfast. Nevertheless, tactical and operational excellence, while necessary, is not sufficient, for the strategic challenges and opportunities that the nation will surely face in the future.

Deception

One of the key capabilities required to create strategic advantage is the ability to deceive one's adversaries about plans, intentions, and actions. Deception should be integral to any major operation or campaign. Technology, no matter how sophisticated and available, cannot erase the need for or utility of deception at all levels of military activity. Yet, deception at any level is extraordinarily difficult, reliant as it is on the close control of information, running agents (and double-agents), and creating stories that adversaries will readily believe. At the strategic level, effective deception requires interagency cooperation that is tied to political policy objectives.

In an era of ubiquitous information access, anonymous leaks, and public demands for transparency, deception operations are extraordinarily difficult. Nevertheless, successful strategic deception has in the past provided the United States with significant advantages that translated into operational and tactical success. Successful deception also minimizes U.S. vulnerabilities, while simultaneously setting conditions to surprise adversaries. Thus, strategic deception capabilities and plans must perforce be highly classified—and buttressed by a strengthened counterintelligence capacity.

Deception cannot succeed in wartime without developing theory and doctrine in peacetime. Success requires understanding the enemy culture, standing beliefs, and intelligence-gathering process and decision cycle, as well as the soundness of its operational and tactical doctrine. In order to mitigate or impart surprise, the United States should develop more robust interagency deception planning and action prior to the need for military operations. For support of the offense, a plan needs to be developed to build up strategic departmental deception activities with the required trade craft, target expertise, and counterintelligence aspects. To be effective, a permanent standing office with strong professional intelligence and operational expertise needs to be established. To support the defense, offensive means should be used to shape and degrade emerging threats.

Avoiding and Responding to Surprise

The Department should pursue several areas to enhance its capability to avoid and respond to strategic surprise. The most pressing concerns involve: red teaming, war gaming, and counter-intelligence.

Red Teaming

Red teams are established by an enterprise to challenge aspects of that very enterprise's plans, programs, and assumptions. Many historical examples of the United States suffering strategic surprise—ranging from Pearl Harbor, to policy objectives unraveling in the aftermath of the Tet Offensive during the Vietnam War, to the rise of counterinsurgency after successful combat operations in Iraq—have two principal origins. The first is the inability or unwillingness of senior

military and civilian leaders to challenge fundamental assumptions underlying their strategies and plans. The second is the U.S. propensity to believe that successful operations are the basis of strategy, rather than the other way around. That is, understanding that operations are only relevant in so far as they implement a comprehensive strategy aimed at achieving a desired political end state. Challenging one's own assumptions is extremely difficult, particularly at the strategic level where the political stakes are high. Therefore, it is critical to establish processes that reduce risks and increase opportunities for success.

A viable red teaming process needs to be more than an *ad hoc* activity. It needs to be a structured process that is executed by skilled and effective team members and that has the strong support of senior leadership. Effective red teams have several key characteristics. The team members must be well educated, analytical, and steeped in the culture of the target, issue, and environment. The red team must be independent of influence from the bureaucracies involved but enjoy the support and attention of senior leadership. And the process is used during operational and/or developmental efforts.

Among the many capabilities of a red team, its members must be able to challenge assumptions during planning, simulate enemy capabilities at a high level of fidelity, create branches and sequels that will stress planning to a point of failure, and then mentor/coach friendly forces from enemy or competitor perspectives.

When conducted correctly, red team efforts should diminish the possibility of surprise; increase the flexibility of thought, planning, and execution on the part of the blue force players; accurately evaluate blue force capabilities; and ensure/upgrade the validity of assumptions.

Red Teaming in DOD

Currently within OSD, red teaming is not consistently used and is not consistently valued. Red teaming simultaneously requires uniquely qualified and proficient participants (red teamers) and requires "blue team" principals to ensure full value of the gaming effort. Furthermore, red teaming is not uniformly accepted as accurate or relevant when based on simulations used in developmental ventures. The challenge of

addressing multiple enemies and environments makes accurate simulation difficult.

DOD's red teaming capabilities can be improved if there is an increase in understanding of the value of red teaming across the Department—something that will likely require the clear endorsement, either by directive or direct involvement of the Secretary of Defense to be taken seriously. It is essential that simulations for both training and development be uniformly accepted and encouraged. Fundamental to this is the requirement for a better trained cadre of red team players and improved simulations of current low- to mid-intensity scenarios.

To initiate these improvements the Secretary of Defense should issue a directive that offers general guidance on the value of red teaming and that promotes the adoption of best practices. In addition, red teaming must be taught at the appropriate level of professional military education. Centers for red team development and support should be established where appropriate.

Strategic Level Red Teaming

Red teaming at the strategic level, if properly employed, can save leaders from becoming captives of their assumptions and visions. As the 2003 DSB task force on DOD red teaming activities noted, effective red teaming promotes "wider and deeper understanding of potential adversary options and behavior that can expose potential vulnerabilities in our strategies, postures, plans, programs, and concepts." Red teams can provide a hedge against the social comfort of "the accepted solutions" and, thus, guard against bias and conflict of interest. Furthermore, at the strategic level, red teams can provide a "hedge against inexperience." To be comprehensive, red teaming must competently perform three key functions: "surrogate adversaries and competitors of the enterprise, devil's advocates, and sources of judgment independent of the enterprise's 'normal' processes."[16]

The selection of strategic level red team members is perhaps the key ingredient in an effective process. They must be highly respected,

16. U.S. Department of Defense, *Report of the Defense Science Board Task Force on The Role and Status of DOD Red Teaming Activities* (Washington D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics) September 2003.

critical thinkers who have credibility within the Department. In many ways, these red team members become mentors and coaches to the senior leaders they are advising. That said, they must be independent, but trusted, agents who are able to step outside of the press of events to provide what in all likelihood will not be popular interventions. Thus, the fundamental role of red team members is to challenge strategic assumptions, not to validate plans.

Currently, at the strategic level (Joint Staff and above) in DOD today, there is an inadequate standing capability to challenge assumptions and visions during strategic planning. There is little ability to quickly and effectively simulate adversary and competitor capabilities at the strategic level. Additionally, there is the ongoing challenge of creating and sustaining consistent interagency participation at the appropriate levels.

Effective strategic red teaming should include a standing body of interagency and extra-governmental teamers chartered to operate independently of "normal" processes. This will require a standing source of current, experienced, and qualified red teamers. This team must focus on a process that explores the possibilities, challenges assumptions and conventional thinking, and stresses the conduct of operations. It must not just validate plans.

To begin this process, DOD should take the lead in creating strategic interagency red teams in the most probable areas of catastrophic surprise (cyber, space, nuclear, and perhaps bio). These efforts must be sustained by a small corps of trained and relevant red team members established by the Secretary of Defense—members with expertise as appropriate to the activity, scenario, or exercise to be evaluated.[17]

War Gaming

War gaming at the strategic level is, in many ways, closely related to red teaming in that it provides an environment within which strategic plans can be "gamed to failure" before actually executed. This involves the very difficult process of translating policy objectives and desired end states into strategic options. Red teaming is a component of this

17. For a detailed assessment of red teaming, see U.S. Department of Defense, 2003.

endeavor; red teamers challenge assumptions, act as a devil's advocate, and provide independent judgment.

Effective strategic war gaming must involve the principals from across the agencies of government to be effective. Only principals have the authority to make the decisions that an effective war gaming process will demand. Additionally, deep interagency player expertise is essential. Absent these "expert" players, others with less relevant knowledge will necessarily embed assumptions beyond their expertise in strategic plans. This is not unlike the situation of DOD planning largely in isolation for operations in post-war Iraq. Quite simply, DOD did not (and should not be expected to) have the necessary resident expertise in governance, rule of law, economic development, and other related areas of expertise. These are the realms of the other agencies of government. Therefore, to develop effective and robust strategic plans that are capable of realizing policy objectives, an interagency approach to planning and war gaming is essential.

Counterintelligence

Defense counterintelligence can and should play a major role in mitigating capability surprise, and the need for unity of command over defense counterintelligence programs and resources is paramount.

U.S. national security depends in significant measure on protecting the critical secrets that give advantage. The compromise of those secrets allows an adversary to shorten its lead time to build capabilities by stealing those of the United States, and to enable countermeasures to defeat or degrade U.S. advantages—all leading to capability surprise. DOD's personnel, operations, installations, and information are principal targets of foreign intelligence interest.

Counterintelligence insights into the targets, tasking, and activities of adversary intelligence services help inform security measures to protect critical national security information and operations. Counterintelligence can expand the set of operational options to shape, deter and defeat emerging threats (*e.g.* through perception management/deception operations). Counterintelligence can also provide insights into foreign

intelligence taskings, which may serve as the earliest indicators of adversary intent.

This study examined a number of domains, ranging from cyber to space to conventional military operations. In each, the vulnerabilities of the United States to foreign (state or non-state) intelligence penetration and exploitation were found to be considerable. Existing U.S. counter-intelligence capabilities are spread throughout the DOD, often *ad hoc*, and weak. This is the case in part because the Secretary of Defense lacks coherent command and control over the Department's counter-intelligence resources, programs, and activities. Defense counter-intelligence was untouched by Goldwater Nichols. As a result, military service counterintelligence components are service-specific—there is no joint operational capability. While the Service components provide counterintelligence support to combatant commands, the command structure is ill-suited to undertake global operations against an adversary intelligence service.

Clearly, unity of effort is a prerequisite for an effective counter-intelligence capability. Nevertheless, a truly comprehensive U.S. strategic counterintelligence capability will necessarily involve other agencies of government and selective private entities. Current counterintelligence deficiencies must be addressed to ensure U.S. capabilities are available to minimize strategic surprise—and to visit surprise on U.S. adversaries.

In 2008, the Under Secretary of Defense for Intelligence (USD (I)) established a Defense Counterintelligence and Human Intelligence Center at the Defense Intelligence Agency (DIA), which is well-suited to analyze the modalities for establishing a joint operational counter-intelligence component within DOD. Perhaps following the U.S. Special Operations Command (SOCOM) model, the new joint command would have the standing mission of degrading foreign intelligence capabilities that threaten U.S. military operations, while retaining the Service focus of the counterintelligence organizations.

To augment this effort, the USD (I) should stand up a short-duration tiger team within this center to work out the modalities to:

- elevate counterintelligence to a joint operational component within DOD with the standing mission of degrading foreign intelligence capabilities
- enable a robust counterintelligence planning function focused on foreign intelligence threats
- study analytic insights to support warning analysis and to inform security programs

Conclusion

Red teaming, war gaming, counterintelligence, and deception are all highly inter-related components of a U.S. strategic planning and execution system that enables our nation to achieve policy objectives, protects from surprise, and creates exploitable vulnerabilities among adversaries. This panel report has endeavored to highlight shortfalls and opportunities in each of these areas—all of which require DOD action and interagency attention—to provide the United States with the capacity to anticipate and mitigate future operational surprise and to enable the nation to both create and exploit asymmetric advantages against any and all potential adversaries. After identifying needed capabilities through these components and processes, the nation must act to prevent, mitigate, or rapidly adapt to future situations and thus to be better prepared for the eventuality of surprise. The space and cyber discussions in previous chapters serve as examples.

Appendix 1-A. Excerpts from the National Space Situational Awareness Roadmap

The Executive Summary from the "National Space Situational Awareness Roadmap" (April 8, 2008) follows:

> This National Space Situational Awareness Roadmap outlines a national strategy to produce space situational awareness capabilities to support our Nation's need for expanding knowledge in the space regime. Increasingly, potential adversaries are employing space and developing asymmetric means of countering U.S. space capabilities. As such, our ever-growing reliance on space requires this Nation to embark upon dramatic improvements of our space situational awareness capabilities to maintain pace with current and emerging threats.
>
> Space situational awareness (SSA) enables decision makers the ability to fully leverage and protect American and allied space capabilities and counter those systems used for purposes hostile to our national interests by leveraging traditional and non-traditional space surveillance, detailed reconnaissance, space intelligence data, synthesis of status, and understanding of space environment impacts.
>
> The 2006 National Space Policy provides guidance and direction for this National Space Situational Awareness Roadmap. The policy directs the Secretary of Defense to conduct SSA for the U.S. Government; U.S. commercial space capabilities and services fused for national and homeland security purposes; civil space capabilities and operations, particularly human space flight activities; and, as appropriate, commercial and foreign space entities. To carry out this responsibility, The Commander U.S. Strategic Command (USSTRATCOM) tasks Command Joint Functional Component Command for Space (CDR JFCC SPACE) to conduct space operation.

The United States must posture its space forces for the future. The SSA capability modernization and strategic investment approach presented in the Roadmap will meet the near-term needs of our Nation, while at the same time ensure the future force structure is relevant (by accomplishing core mission threads), capable and sustainable. Our Nation must transform space situational awareness capabilities to a more agile, precise, capable force by following a strategy of integration, net-centric architecting, selective service life extensions, procurements and retirements to solve the critical recapitalizations/modernization challenge. This Roadmap defines a plan, in step with validated, prioritized USSTRATCOM Joint Capabilities Document SSA requirements, to solve recognized shortfalls in our ability to integrate data, leverage the spectrum of contributing assets, fill gaps in sensor coverage, timely characterize of objects in all regimes, and track small objects. The future of Space Situational Awareness and Space Operations will require a comprehensive global effort, integrating and leveraging capabilities across all the Department of Defense, Intelligence Community, Civil, and Commercial and Foreign entities.

Part Two.
Technological Surprise

Chapter 2-1. Introduction

The Technology Panel of the Defense Science Board (DSB) 2008 summer study addressed the technology aspects of capability surprise. The panel began its work with the core assertion that capability surprise includes novel use of existing technology or system integration of a new technical idea. The panel examined the technology landscape before proposing a framework for technology discovery and innovation. An assessment of prior examples of technology surprise, and evaluation of best practices in industry and government responses to technology surprise informed our recommendations.

Over the past decade, a global research community has emerged that has flattened the barrier to entry for technology access and exploitation. The private sector has recognized this phenomenon and has shaped its global research and development efforts to include significant off-shore elements. Because the Department of Defense (DOD) and the intelligence community have limited access to off-shore technology development, they rely significantly upon the contractor base for technology discovery and exploitation.

Understanding the early and weak innovation signals resulting from this discovery activity is key to accurate projection of emerging capabilities. A few key researchers in the right field can have an enormous impact. New horizon scanning and technology watch tools, based upon social network analysis, are beginning to appear that provide cueing to these weak signals. The recommendations of this panel integrate this concept into a decision support framework to provide emerging capability assessment and candidate countermeasure options for action.

Chapter 2-2. The Global Technology Landscape

The global technology landscape has changed significantly over the past decade.[18,19] As a result, many countries and transnational organizations have ubiquitous and rapid access to leading edge technology across many disciplines. Furthermore, as the infrastructure of India and China mature, they are beginning to draw upon their respective populations of 1,148 million and 1,330 million to challenge U.S. technical capabilities.

While these trends influence many dimensions of U.S. policy, they also underlie the increasing scope and tempo of global innovation and more ubiquitous access potential adversaries may have to emerging technologies. They also provide insight into early technology development signatures and precursors. This report draws on data and ideas developed by consideration of these larger issues, but concentrates on the smaller purpose of establishing recommendations for how DOD might anticipate, mitigate, and respond to threats to national security posed by increasing levels of foreign technical capabilities.

Framework for Technology Surprise

A small group of people with access to the right resources and unconstrained by conventional approaches can create technological surprise across many fields. One example of such a surprise is shown in Figure 2-1. The incumbent conventional thinking at the time placed the development of aircraft many years in the future.[20] The Wright Brothers were undaunted by the investments and infrastructure that Samuel Langley had massed. They approached the challenge through innovation and numerous flight trials, and eventually succeeded in demonstrating

18. Thomas L Friedman, *The World is Flat* (New York: Farrar, Straus, and Giroux, 2005).
19. National Academy of Sciences, *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future* (Washington, D.C.: National Academies Press, 2007).
20. *New York Times*, "Flying Machines Which Do Not Fly," October 9, 1903.

powered flight—a success witnessed by only five other people present for that first flight. This milestone, though a surprise to many, was preceded by numerous technical demonstrations and accomplishments.

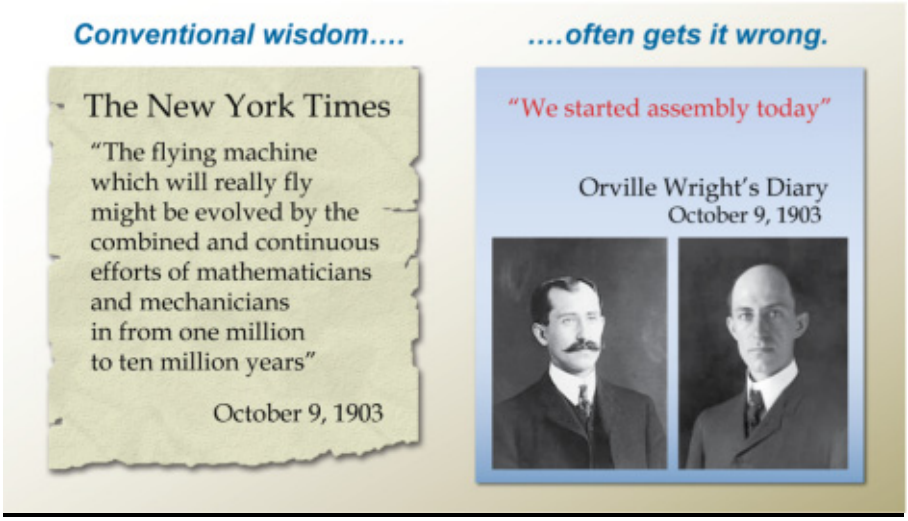


Figure 2-1. The Wright brothers' construction of a powered, heavier-than-air craft surprised many established experts by creating an unexpected technical capability.

Identifying those initial signals of invention and innovation is key to the framework for technology surprise, as shown in Figure 2-2. This model is based on the view that much innovation is driven by small groups of researchers distributed globally with ubiquitous access to technology. This environment generates "innovation signatures" that range from tangible, physical devices such as published work and prototype products, to less tangible, intellectual artifacts such as speeches and social connections. These signatures can be correlated, combined, and condensed into plausible descriptions of the state of foreign technical capabilities. **Threat assessments** invoke additional understanding of political objectives and social constraints to determine, in a prioritized way, the impact those foreign capabilities might have on U.S. national interests. **Option analyses** examine, in a multiplayer, nonzero-sum game-theoretic framework, potential U.S. responses to those threats. These options include open methods to influence foreign initiatives, such as diplomatic initiatives (*e.g.*, test ban

treaties), or more covert efforts to obtain additional signature data that could reduce ambiguities about the state of affairs.

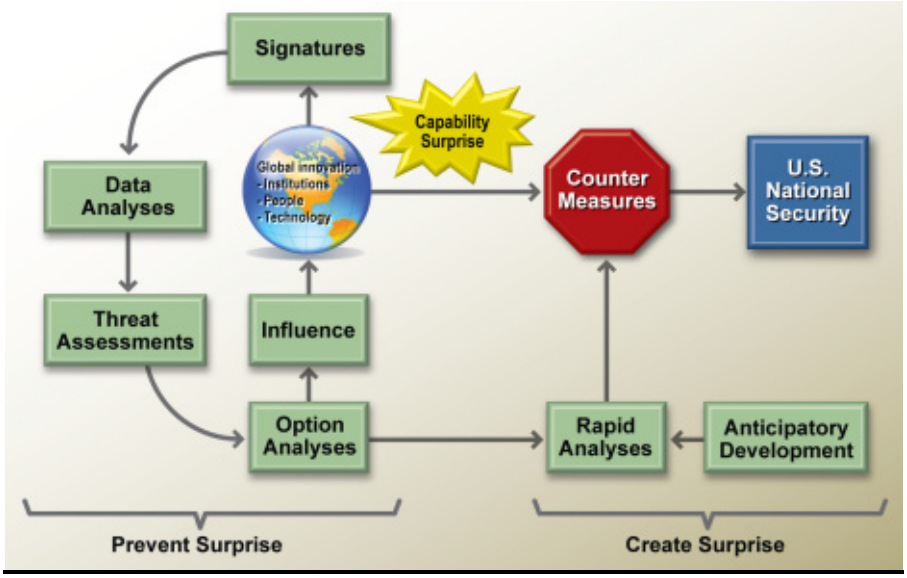


Figure 2-2. The processes needed to detect and prevent technical surprise are similar to those used to manage uncertainty in other changing environments.

The technology surprise framework includes a path to create capabilities that surprise U.S. adversaries. Development of prototype technical countermeasures in anticipation of emerging adversary technical capabilities, carried out in secure environments, is a demonstrably effective mechanism to outperform an opponent, even if the United States is the first to be surprised. The rapid deployment capability is targeted at converting these technical prototypes to fielded military capabilities well ahead of, and in some cases to respond quickly to, the adversary. The resulting framework allows the United States to detect technology development precursors, both to respond to and to generate capability surprise.

Sources of Technology Surprise: People, Institutions, and Relations

Technology surprise takes place in a context of collaboration, funding, intellectual property protection, security, recruiting, mergers

and acquisitions, and other similar activities. As a result, conventional approaches of geospatially focused detection need to be supplemented with new techniques.

Frequently, the space of technical innovation has been described by domain taxonomies: nested lists of domains and sub-domains.[21] While quite useful in support of planning and budgeting, these are less useful in the context of detecting technical surprise in a world where innovation may occur in groups who are not bound to conventional approaches that have been used in the past and who are much more globally interconnected than ever before.

Instead, Figure 2-3 offers an initial visualization of the landscape of technical innovation. The central premise is that the common element of innovation is *people* and the relationships among them, both institutional and social, through which flow ideas, experience, funds, and access to end-users.

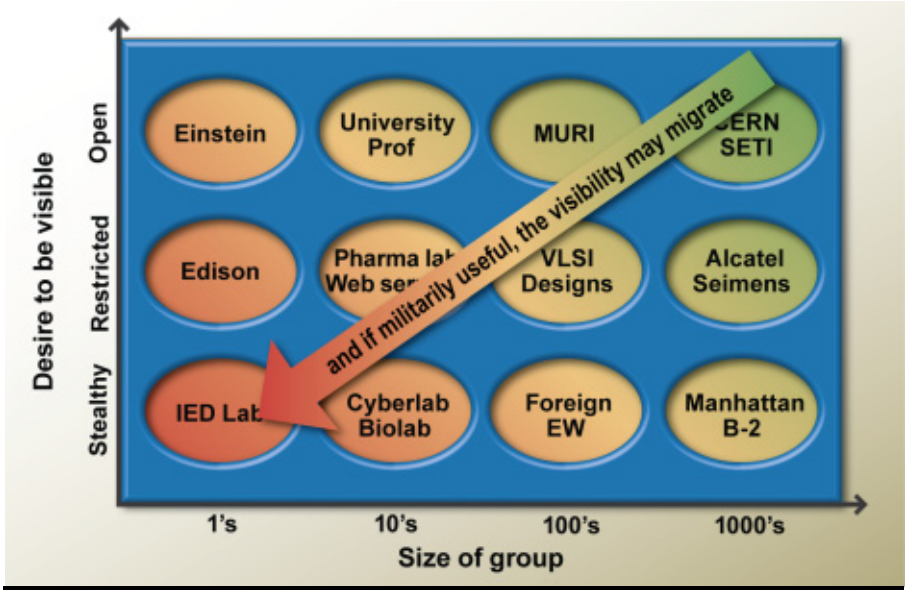


Figure 2-3. Surprise is created by groups of people, some in the open, some in deep hide, all interconnected.

21. For example, the *Defense Technology Area Plan* as once published by the Director of Defense Research and Engineering.

This landscape can be characterized by the size of the core group working on an innovation and the desire of that group to have their work exposed to other communities. At one extreme is the high energy particle physics research community, with thousands of members spread over the globe (though currently focused on the Large Hadron Collider) and who publish thousands of papers every year in open journals. At the other extreme are the fabricators of improvised explosive devices (IEDs) in Iraq, who operate on their own and have no desire to be observed by any more than a handful of associates. In between are groups of various sizes who only want to reveal part of their capabilities, often because they wish to preserve some competitive (business or military) advantage through protection of intellectual property, trade secrets, or business plans.

None of these groups operates truly alone. Over the course of their careers, their members migrate through many different institutions—schools; industry; government; or social, religious, and/or ideological groups. In each of these roles, they establish additional relationships through learning, collaborating, and mentoring other people, and through sponsoring, delivering, and facilitating other technical projects.

The central thesis is that technical surprise is far more likely to arise from activities in the lower left of this diagram, rather than from the upper right. Large technical projects that publish widely are easy to observe and assess. Small groups that deliberately want to hide are far more likely to spring a surprise. Because of the low capitalization requirements and small labor force needed, IED fabrication, offensive cyber activities (hackers and others), and genetic sequencing labs for bio-warfare rank high as activities with the potential to surprise. However, many others are possible.

Because of their high potential to create surprise, groups in the lower-left area of the figure are targets of interest for this study. The question is, how many of them might exist and how might they be discovered?

The Changing Demographics of Technology

According to the most recent data from the Organisation for Economic Cooperation and Development (OECD), 2002 saw approximately five million full-time-equivalent researchers at work throughout the globe—only 25 percent of whom were in the United States.[22] The same year saw 3.5 million new graduates with science and engineering degrees (undergraduate, not including community colleges and associate degrees), only 12 percent of whom graduated in the United States. Globalization of the technical community is a fact, and, due to the spread of knowledge and educational institutions, the rate of growth of the offshore technical population is now almost proportional to the rate of growth of the offshore population as a whole.[23] Figure 2-4 illustrates these numbers, with particular emphasis on the rapidly changing postures of China, India, and the Russian Federation.[24]

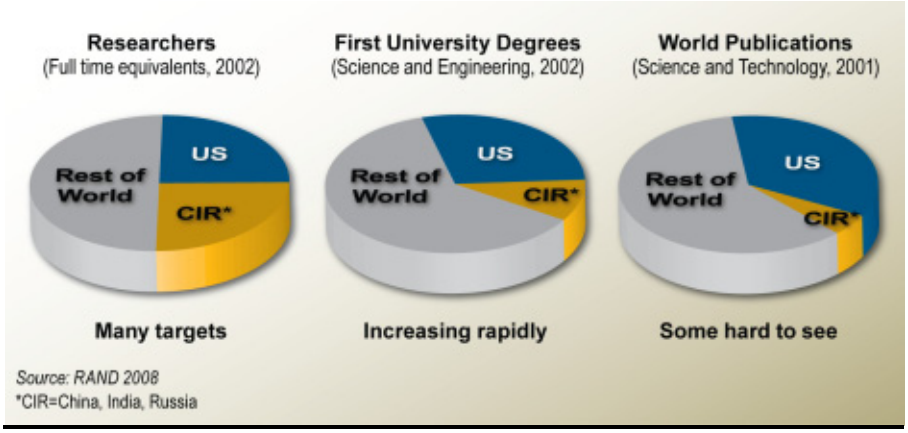


Figure 2-4. The number of people offshore, capable of creating technical surprise, is large, growing, and sometimes hidden.

22. Organisation for Economic Cooperation and Development. *OECD Science, Technology and Industry Outlook* 2002. Available at http://www.oecd.org/document/19/ 0,3343,en_2649_34273_1962451_1_1_1_1,00.html (accessed June 2009).
23. Richard B Freeman, *Does Globalization of the Scientific/Engineering Workforce Threaten U.S. Economic Leadership?* NBER Working Paper No. 11457 (Washington, D.C.: National Bureau of Economic Research) July 2005. Available at http://www.nber.org/papers/w11457 (accessed June 2009).
24. Galama and Hosek, *U.S. Competitiveness in Science and Technology* (Santa Monica, Calif.: RAND National Defense Research Institute, 2008).

The activity of admission committees for U.S. science and engineering graduate schools has challenged the conventional wisdom that foreign undergraduate educational institutions are of lower quality than those in the United States. In 2006, more U.S. PhD degrees were awarded to students from Tsinghua and Peking Universities than to students from any American school.[25] The increasing number and quality of foreign graduate students, a significant fraction of whom return home after receiving their degrees, have become significant challenges to the U.S. technology superiority upon which much of the nation's economic and military security leadership has been based.

Not every undergraduate will attempt to create a technical surprise that will endanger U.S. national security. But a few will. One way to prevent surprise will be to identify these few early, and track their research. This is the role of the horizon scanning and technology watch elements that are described later in this report.

A key target of a technology watch effort is the significant change that is underway in the cultural landscape, as outlined in Figure 2-4. Chinese, Indian, and Russian scientists publish considerably fewer articles in scientific journals than do their American and European counterparts.[26] The United States has limited visibility into technical efforts in those countries where the potential for growth in technical innovation is greatest. However, the private sector is mining these areas and provides an opportunity for broader technical engagement and understanding.

25. Jeffery Mervis, "Top Ph.D. Feeder Schools Are Now Chinese," *Science* 321, no. 5886 (July 2008). Available at doi:10.1126/science.321.5886.185 (accessed June 24, 2009).
26. Richard B. Freeman, "Globalization of the Scientific/Engineering Workforce and National Security," in *Perspectives on U.S. Competitiveness in Science and Technology*, Titus Galama and James Hosek eds., 2007. Available at http://www.rand.org/pubs/conf_proceedings/CF235 (accessed June 24, 2009).

Chapter 2-3. Historical Examples

To provide a foundation on which to explore the issue of technical surprise, the panel investigated, in some detail, both the reasons for and responses to many historical cases of technical surprise. Several of the most relevant examples are described in this chapter.

Sputnik

On October 4, 1957, the Soviet Union successfully launched the world's first artificial satellite, Sputnik I. The United States was not surprised that the Soviet Union launched a satellite, but rather that they launched a satellite before our nation did. This launch validated the perception of a technology gap between the United States and the Soviet Union. In addition, the public feared that the Soviet's ability to launch satellites demonstrated the ability to launch intercontinental ballistic missiles that could reach the U.S. homeland.

Indicators

The fact that the Soviet Union was going to launch a satellite should not have been a surprise. The technological feasibility of producing an artificial satellite had been published in a 1946 RAND report. Following this report, both the United States and Soviet Union began programs to develop artificial satellites. In 1952, the International Council of Scientific Unions established July 1957 through December 1958 as the International Geophysical Year (IGY) and, in 1954, adopted a resolution calling for artificial satellites to be launched during the IGY. Both the Soviet Union and the United States responded to the call by announcing their intent to build and launch satellites during that time. The Soviet Union immediately began building a simple satellite, modifying R-7 rockets for launching the satellite and developing the required stations. In early 1957, a number of Soviet announcements and articles were released, promising an on-time satellite launch and even publishing frequencies on which the satellite signal could be heard.

Reasons for the Surprise

Despite these indicators, the United States assumed that it would still be first to launch. However, the U.S. satellite program remained a low priority effort and, mirror-imaging our own thoughts and objectives, it was assumed that the Soviet Union placed a similar low priority on a satellite launch. The United States underestimated the Soviet Union's view of the prestige associated with the satellite launch. In fact, launching on time was so important to the Soviets that they settled for a smaller, simpler satellite in order to maintain the launch date. Additionally, the United States did not believe the Soviets had the ability to take the required steps more quickly and cheaply than our nation could. Thus, because the United States was unable to view Soviet strategies and priorities through their value structure rather than our own, and because a bit of arrogance led us down the road of "they can't do that," the surprise was, to a large degree, self-inflicted.

After the Surprise

The Sputnik launch kicked off a number of immediate actions aimed at increasing U.S. technological capability and avoiding similar surprises in the future. First, high priority was placed on a U.S. launch and a new satellite program was funded, resulting in the launch of Explorer I four months later. The United States created the National Aeronautics and Space Administration (NASA) to mobilize U.S. resources in the space race and the Advanced Research Projects Agency (ARPA) [now the Defense Advanced Research Projects Agency (DARPA)] to research new technologies that were considered important but "risky." The United States also passed the National Defense Education Act, which reformed science and mathematics education and provided incentives for science, technology, engineering, and mathematics degrees.

Soviet Bio-weapons

The development of the Soviet biological agent capability was rapidly accelerated in the 1970s, shortly after the U.S. unilateral declaration that it would cease development of biological agent weapons. In 1969, President Richard Nixon made the decision to cease research and development of offensive biological warfare activities because of the

massive nuclear capability available and because the predictability of effects of biological threats on a specific target was wanting. In 1972 an international agreement, the Convention of the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxic Weapons Convention (BWC), was adopted. The sudden outbreak of anthrax cases in Sverdlovsk (now Ekaterinenberg) in 1979 led to concern about adherence of the Soviet Union to the BWC. During the 1980s and early 1990s, the capabilities of the former Soviet Union became more clearly understood. Programs related to the properties of viruses that cause hemorrhagic fevers were established at the Belarus Research Institute for Epidemiology and Microbiology (BRIEM) (Minsk) and of bacteria that cause a variety of human and animal diseases in Kazakhstan. Diseases of plants were examined at several other facilities in the former Soviet Union.

Indicators

The existence of the technology associated with biological warfare was certainly no surprise to the United States. Biological warfare has been employed since 300 BC when decaying corpses of infected animals and humans were placed near water and food supplies of adversaries. Diseases such as plague and smallpox were among agents that were actually collected and employed against adversaries. World War I saw the development of biological warfare strategies. Cholera and plague were thought to have been used in Italy and Russia while anthrax was believed to have been used in Romania.

The Geneva protocol of 1925 (Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases and of Bacteriological Methods of Warfare) banned the use of biological agents in warfare but not the research, development, production, or stockpiling of such agents. Single cell production equipment was manufactured by Soviet allies and did not require western technology. Weaponization was also reasonably well-developed during World War II and included advances in lyophilization and properties of particulate dispersion for bacterial weaponization. Both the United States and the Soviets shared the perceived need to develop an offensive response to each other's emerging capabilities and pursued bio-weapons programs.

Reasons for the Surprise

In 1972, the United States assessed biological agents to be highly unpredictable, uncontrollable, and politically infeasible in the context of the Vietnam War. In response, the United States abolished its program and threatened nuclear response against those electing to employ biological agents. America also assumed that the Soviets would come to the same conclusion with regard to biological agents. By publically announcing U.S. intentions to abandon bio-weapons, the United States believed that the Soviets would have no reason to continue their program. Our nation also believed that the strong nuclear capabilities of the Soviets would make it unnecessary for them to develop bio-weapons.

The Soviets, on the other hand, assumed that the public announcement of the abolishment of the U.S. program and the disappearance of any visible activity simply meant that our program had gone "black," perhaps because of some breakthrough. This lead to an increase in Soviet activity, the opposite of what the United States had assumed would be the result. Thus, even in terms of the Soviet Union—a potential adversary that the United States studied continually and in-depth—failing to fully "understand the adversary" was a factor in generating surprise.

After the Surprise

As the central government of the former Soviet Union diminished in strength at the end of the 1980s, the United States and other western governments made efforts to redirect scientists working on biological weapons development in the former Soviet Union into other areas of research. These efforts were facilitated by funds from the Department of Defense, nongovernment organizations, and other national entities. Scientists from BRIEM (Byelorus), Vektor (Kazakhstan) and other biological weapons facilities visited the West and Soviet facilities were opened to the United States. However, these steps did not keep bioweapons expertise from spreading to other countries (*e.g.*, Iraq).

Stealth: A Surprise Created by the United States

The history of the development of long-range surveillance and bombing aircraft is intimately coupled to the development of air

surveillance radar to detect those same aircraft. It was a true "cat and mouse" game that was carried out on a global scale over 60 years, initially during World War II between the United States and Germany. After the war, there was a 30-year hiatus as the victorious United States focused on other technical developments. The final emergence of modern U.S. stealth aircraft was a large-scale capability surprise that the United States sprang on the Soviet Union. It mitigated a key military advantage of the former Soviet Union and recaptured the third leg of the U.S. nuclear triad to hold at risk the key assets of the Soviet Union.

Engineering the Surprise

Beginning in the 1930s, U.S. aerospace engineer Jack Northrop, inventor of the internal strut wing that revolutionized aircraft design, was at work creating flying wing aircraft that promised greater aerodynamic efficiency and reduced radar signature due to their swept wing design. They were constructed of aluminum skins on a steel frame and did not employ any materials designed to minimize radar backscatter. While the shape of a flying wing was recognized as being of lower radar signature, little attention was paid to the optimization of this characteristic and it was only realized as an afterthought, beginning with the N9Mb and ending with the YB-49 in 1950s (Figure 2-5).

In Germany, the aircraft developers at Horton Brothers were experimenting with their first flying wings, following in the footsteps of Jack Northrop. Their designs matured and by the 1940s the Horton HO IX V2 (GO 229) had a range of 1,500 kilometers carrying a 1 kilogram payload. In 1944, the German government's Reich Air Ministry (RLM) issued a requirement for an aircraft with a range of 11,000 kilometers (6,835 miles) and a bomb load of 4,000 kilograms (8,818 pounds). The bomber envisioned was to be an Amerika Bomber, with the capability to fly from Germany to New York City and back without refueling.

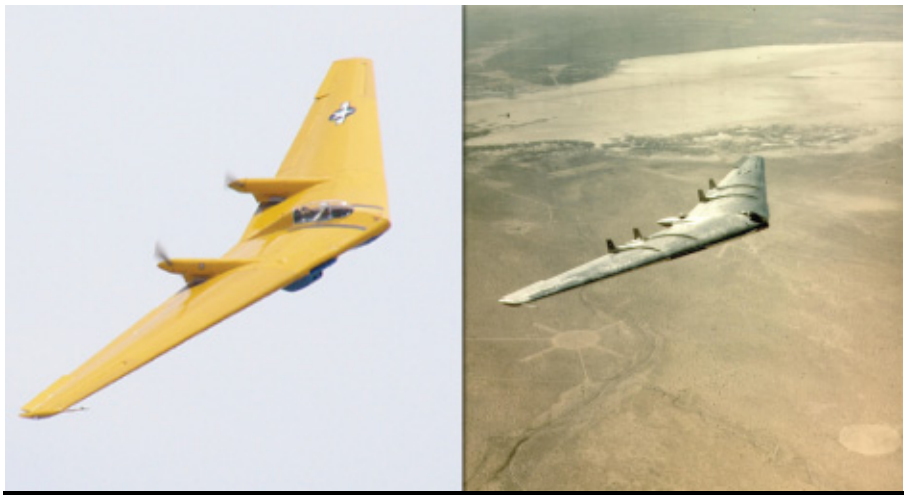


Figure 2-5. Northrop's N9Mb and YB-49

Five of Germany's top aircraft companies had submitted designs, but none of them met the range requirements for this Amerika Bomber. The Hortens, who had a built the Horton HO XVIII (11,000 kilometer range, 4,000 kilogram payload) (Figure 2-6), were not invited to submit a proposal because it was thought that they were only interested in fighter aircraft. Yet, they could have met the requirements. By the time that fact was recognized, it was too late—the Allies were approaching the Rhine.

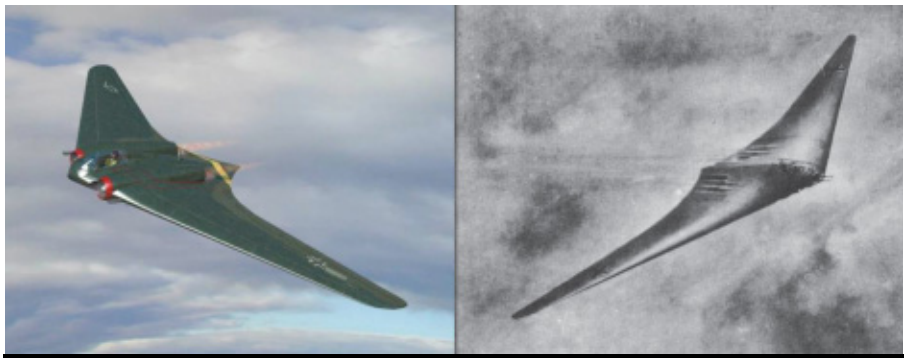


Figure 2-6. Horton HO IX V2 and HO XVIII

The German HO XVIII design was complex and employed both radar absorbing paint ("Schornsteinfeger" [Chimneysweep]) and radar absorbing structure (wood, carbon black, and beeswax). The fortuitous use of wood for aircraft by Horton was originally driven by the unavailability of metals in Germany during the war and enabled the design of complex multilayered radar-absorbing wood aircraft structures. The complex and integrated stealth aircraft as represented by the last HO prototype would not be exceeded until the reemergence of stealth technology in America in the 1970s.

By the early 1970s, Lockheed and Northrop were the two aerospace companies that had organized small “skunkworks” organizations to push the limits in aircraft designs and use rapid prototyping to create cycles of “build/test/learn” quickly. Northrop’s “Observables” group, which developed the skills and tools to analyze and design aircraft with specified radar, electro-optical signatures, was all but disbanded in the early 1970s, but kept alive by the sponsorship of a senior executive, Donald Hicks (later to become Under Secretary of Defense for Research and Engineering). The early research was focused on simple flat-faceted designs that had poor aerodynamic performance but good low observables performance.

Competing designs were developed by Northrop and Lockheed and subscale prototypes were developed and a winner was chosen. The government’s interest and funding of these game-changing designs was kept under tight wraps by operating under “black program” security rules. The government security rules kept the contracting, existence, and execution of the programs out of the public eye. Even the static radar pole measurements and flight testing were conducted at remote sights, at night, and under a “no full moon” rule.

Lockheed won the DARPA-Air Force Have Blue program competition for a small fighter bomber and was awarded the follow-on full-scale development program which led to the flat facetted design of Dennis Overholser, the F-117. Northrop went on to win the DARPA Tacit Blue program to develop the next generation of stealth aircraft with their continuous curved surface designs. The competitive landscape was then set for the ultimate prize, the Advanced Technology Bomber, B-2 whose mission was long-range, penetrating nuclear

bombing deep inside the Soviet Union (Figure 2-7). Northrop went on to win that contract using its continuously curved surface stealth design, tailless flying wing, fly by wire, and heavy use of structural radar absorber. The design was evolutionary beyond the YB-49 and the HO-XVIII and yet revolutionary in its capability.

Figure 2-7. B-2 Spirit

Impact of the Surprise

The mission envisioned for the B-2 was bold: to make obsolete and defeat the extensive Air Defense Radar Network surrounding the former Soviet Union, a system that took 20 years and billions of rubles to perfect. The Integrated Air Defense Network was the pride of the Soviet leadership and one which they believed impenetrable to U.S. air forces.

From 1960–1980, the Soviet Union ringed Moscow with a continuous and overlapping low frequency surveillance radar perimeter coverage. Figure 2-8 shows in red circles a prototypical ring of radars. The integrated air defense network complemented the surveillance radar with SA-6 and SA-10 radar guided missile interceptors that were cued to the radar targets. The U.S. strategic nuclear bomber leg, as represented by the B-52 Stratofortress, was at risk. The B-2 was designed to reduce each radar's detection range by a large factor and, thus, create holes in the continuous radar coverage and reopened integrated air defense network.

Figure 2-8. Notional Surveillance Radar Perimeter Surrounding Moscow

Key Insights

A number of insights can be drawn from these historical examples. The most obvious insight is that **we, as a nation, will be surprised**—especially in the context of the technology globalization documented previously in this report. However, technology surprise does not result only from creating or modifying technology. It also results from combinations of vision, opportunity, decision, action, and—in wartime—simply from lessons derived by an opponent from field experience.

In the two example cases where the United States was surprised, the surprise did not occur because of lack of awareness or understanding of technology. In both cases, had national leadership established different priorities as a result of better understanding the adversary or being more open in assessing adversary capabilities, the surprise could have been avoided or significantly lessened. Information on the relevant technologies had been published in open literature and was well known. Lack of intelligence was not the main contributor. In each case, the United States was aware of the adversary's activities. The main cause for surprise was that the United States failed to understand the values, capabilities, and priorities of the adversary. We, as a nation, assessed that the adversary's values and priorities would be a mirror image of our own.

Additionally, our nation failed to accurately assess the impact that the events would have on the United States. In the case of Sputnik, the United States was also unable to envision a transition from technology to capability faster than the norm. The ability to anticipate and/or to counter surprise in the future will depend on a U.S. ability to accurately assess the risk and likelihood of a threat and will require intelligence fusion of technical, developmental, operational, and cultural expertise, as well as the ability to pull the information together in a strategic framework that the adversary could employ.

Of course, these historical examples do not reflect the changing demographics of the global science and technology enterprise. These changes will do nothing to decrease the risk of mischaracterizing opponents' goals and timelines. However, they will increase the potential for pure technical surprise as well—unless the United States increases its efforts to monitor progress in foreign technical institutions.

Given these insights, it is difficult to firmly predict the next sources of surprise. However, the United States can look at trends, and compare impact, cost, and visibility of foreign investment in general domains. For example, Figure 2-9 shows the cost of entry versus consequence (or impact) of some representative technology domains. The risk/benefits of the different technologies range from low cost of entry, low impact events that affect a few people, like criminal activities or hacker attacks; to high cost of entry, high impact events, such as a nuclear strike.

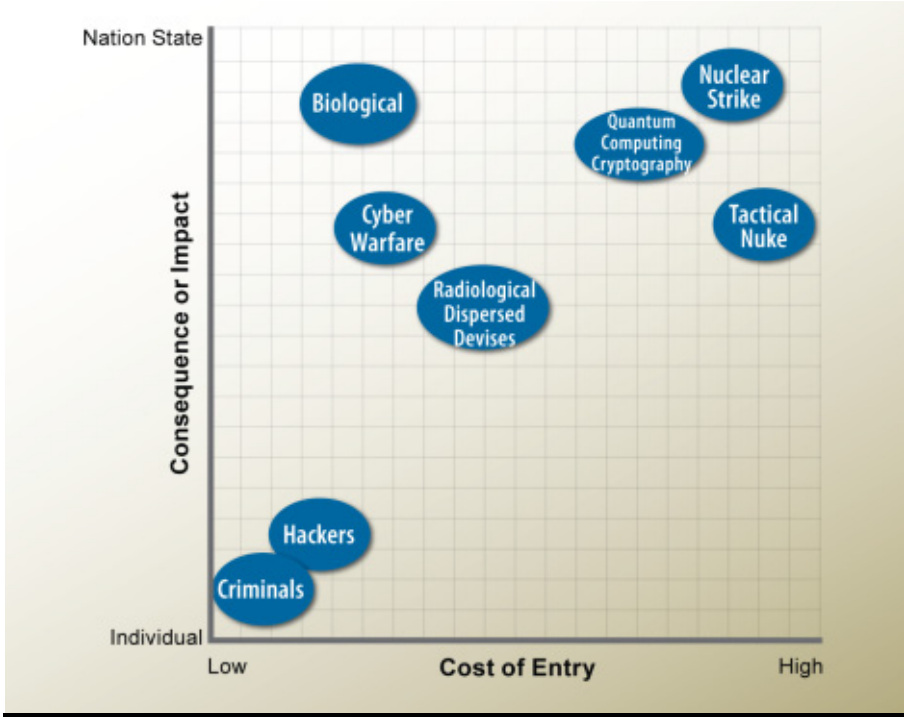


Figure 2-9. Risk/Benefit Analysis for Future Threats

Chapter 2-4. Current Practices for Technology Assessment

To understand current best practices, the panel interviewed representatives both from major U.S. industrial organizations and from key government organizations that are charged with competitive assessment and technology tracking. The results of these interviews were used to inform the panel recommendations for how DOD should develop a program of technology and horizon scanning to anticipate technology surprise.

Industry Practices for Technology Assessment

The Technology Panel received input on technology assessment practices from a number of industrial firms who compete in the global technology market. These include General Electric (GE), Microsoft, Promega (a mid-sized biotech company), Lockheed Martin (the Skunk Works), Boeing, and In-Q-Tel. Summary comments from these briefings are related below.

GE Global Research has the role within GE of discovering new technology opportunities and spreading them across the businesses. They enjoy strong support from GE CEO Jeff Immelt. They view innovation as a process, and have an annual cycle that promotes interaction among their businesses, customers, and partners.

GE, Microsoft Research, and Promega all have a strong global presence. GE has major research facilities in the United States, China, India, and Germany, where U.S. and foreign scientists and engineers work side-by-side. Not only does this give GE access to the best talent across the world, but it helps them understand regional developments, markets, and culture. Microsoft also has major labs located worldwide—in the United States, United Kingdom, India, and China. A primary role of this organization is to help create and sustain a vigorous intellectual atmosphere in the company, and to seek great new ideas for the business. Promega, a midsized biotech company, is globally located and provides equipment and supplies to laboratories worldwide. Each of

these organizations uses its international presence to maintain active links with leading universities and researchers so that they have an explicit global input and perspective to their technology scanning activities. However, they focus more narrowly on those technologies that impact their business interests.

Lockheed Martin's Skunk Works is a separate advanced development organization with a long track record of fielding innovative aircraft. They attribute much of their success to the philosophy, culture, and processes that have been established, including strong leadership, accountability, and minimization of bureaucracy. Boeing Phantom Works is a central research and development (R&D) and advanced systems development group focused on creating next-generation capabilities. Its independence from the core programs and dedicated focus on the future gives the organization the ability to question traditional paradigms to create innovation. In-Q-Tel is an organization sponsored by the Central Intelligence Agency that uses the venture capital model to seek and support new technology and innovation.

While differences existed in each company's approach, some common threads emerged from these discussions:

- A number of these firms increasingly are locating labs and researchers globally. Among the benefits these firms garner from their global research presence is access to high value intellects worldwide, broad knowledge capture, and understanding of culture and markets in the region.
- These companies have a variety of strategies for finding and creating new and/or disruptive technologies including R&D within operating units and selected acquisitions. In addition, a number have created separate organizations for this purpose (Lockheed Martin Skunk Works, Boeing Phantom Works, and GE Global Research) to free them from mainstream organizational biases, bureaucratic constraints, and conservatism.
- The primary focus of the commercial firms is on current and adjacent markets for new products and services. This helps create focus for their technology activities.

- The companies have structured processes that operate on an annual cycle to link markets, customers, competitors, and technology. These activities are joint between the research organization and the operating organizations.
- Finally, but perhaps most importantly, technology assessment, adaptation, and integration are successful because the top executive "cares"—he or she sets this as a top organizational priority.

Government Practices for Technology Assessment

Government organizations also engage in technology assessment and technology watch activities. These include several agencies in the intelligence community, the Office of the Director, Defense Research and Engineering (ODDR&E), DARPA, as well as other governments (*e.g.*, Defence Science and Technology Laboratory (Dstl) in the United Kingdom). Activities relevant to surprise management include:

- The Office of the Director of National Intelligence (ODNI) is proposing a strategic planning committee with participation from the National Intelligence Council; the Departments of State, Treasury, and Homeland Security; the Office of the Secretary of Defense; and the National Security Council to coordinate approaches to capability surprise.
- The ODDR&E has a technology warning process as well as a number of ongoing initiatives to identify potential areas of surprise from technology development. These include the X2 process, which is a comprehensive approach that draws from a broad community and arrays information in a multidimensional way.
- The goal of the National Ground Intelligence Center (NGIC) Techwatch program is integrated threat assessment. This effort is based on scientometric analysis, an emerging methodology for understanding technology advances at early technology readiness levels.

- The Intelligence Advanced Research Projects Activity (IARPA) approach to understanding technical advances and creating surprise was examined. Critical to this approach is the establishment of a strong program manager culture and a strong focus on areas of relevance to the intelligence community.
- The UK's Dstl (part of the Ministry of Defense) has efforts ongoing in technology watch and technology horizon scanning. Their approach incorporates future strategic context (political, social, economic, technical, legal, and environmental), geopolitical scenarios, force structures, R&D plans, and potential new capabilities of opponents in its analyses. Tight and continuous coordination between intelligence and science and technology (S&T) is an important element of their process.
- Office of Naval Research (ONR) Global serves as a technology watch effort in the U.S. Navy. The program seeks to access and understand emerging trends in the global technology movement and leverage global technology insights. Its aim is to influence the Navy S&T strategy using a broad set of tools to directly engage the international S&T community. Elements of the program include a visiting scientist program, conferences, international cooperative S&T opportunities, bilateral and multilateral agreements for government and military exchanges, and direct research grants and exchanges. ONR Global also reaches out to external groups that help canvass the world for cutting edge S&T.

A number of important observations were derived from the presentations received by the panel on these efforts. In many cases, the presenters were aware of limitations or shortcomings of current approaches and were open in sharing these with study participants. A summary of these observations include:

- There is a general acceptance that a common past approach—creating "lists of lists" of technology threat areas—is not useful or sufficient.

- There is a proliferation of new approaches being tried:
  - They include horizon scanning and delta scanning, techwatch, and X2 (combining data, forecasts, and scenarios).
  - All propose the use of red/blue team exercises, but details are lacking on how this should be implemented.
  - None indicate the use of experimentation to validate models and predictions, or to create surprise (except for DARPA, discussed in the next section).
  - Key uncertainties remain regarding scaling of proposed approaches and the validity of resulting forecasts.
- There is a general acceptance that successful approaches will require (and, therefore, must facilitate) collaboration across intelligence, operations, and S&T communities.
- All recognize that this is a "wicked" problem (see Appendix 2-A, of this report), but no clear DOD focus is apparent.

Creating Surprise: The DARPA Model

DARPA's mission is to prevent technology surprise by creating it. This agency has been very effective in fulfilling its mission by following a strategy that seeks high-risk, high-potential-payoff technologies and military concepts. These projects usually involve 1) technical innovation and creativity and 2) a willingness to challenge developers with very difficult (DARPA "hard") problems.

Much of DARPA's success and longevity is due to the fact that it has been consistently protected by Congress and DOD leadership while, at the same time, being allowed to act as an independent agency without needing to tune its research to formally established military requirements.

DARPA's strategy is to avoid technology surprise by "inventing" new defense technologies. Its approach is to bridge the "valley of death" in funding that often occurs between basic research and the successful application of high-risk, high-impact technology by focusing attention on very difficult problems and by having a high tolerance for failure. It has

been, and continues to be, acceptable for DARPA projects to fail because it understands that an unbroken record of continued success would indicate that the organization is not pushing the envelope far enough.

The concept of operations at DARPA embodies flexibility and opportunism, keeping the agency on the leading edge of technology, and quickly exploiting new inventions, ideas, and concepts with potential military utility. DARPA owns no infrastructure and relies on its program managers, who are frequently rotated, to provide the necessary link to the global research community and to constantly refresh the "DARPA gene pool."[27]

Idea creation at DARPA derives both from "military pull" and "technology push" viewpoints:

- Military pull:
  - maintain a 20 year vision of military capability
  - apply current technology (e.g. joint capability technology demonstrations, advanced technology demonstrations)
  - identify and pursue technology deficiencies arising from the 20 year vision
- Technology push:
  - invest in areas of potential high payoff
  - exploit technology to enable new or greatly enhanced military capabilities
  - focus on long-term technology development

Insights Developed from Industry and Government Best Practices

Combining insights from industry and government, the panel identified the following best practices:

27. For further discussion see the report of the *Defense Science Board Task Force on the Roles and Authorities of the Director of Defense Research and Engineering* (Washington D.C., Office of the Under Secretary of Defense for Acquisition, Technology and Logistics) October 2005.

- Any successful approach to technology assessment requires strong support and involvement from the top of the organization—preferably the chief executive.
- A senior executive needs to be responsible for technology assessment—to lead the activities, to serve as the focal point for promoting interchange, to establish the evaluation process, to draw conclusions, and to decide and act.
  - A strong communications process is required among the involved constituencies.
  - For industry, this includes technologists, developers, customers and marketers. The DOD analog is technologists, developers, operators, and the intelligence community.
- Current government approaches lack processes to connect technology advances with capability threats for emerging threat areas (for example, bio, cyber, and low-grade commercial).
- Frequent experimentation and rapid prototyping are keys to maintaining core competencies, and must be institutionalized. These skill areas include designing and conducting experiments, engineering, and red and blue teaming.
- Occasional failure should be expected, indeed embraced, as an opportunity for learning. If not present, then the organization is not taking sufficient risk.
- There needs to be a process for transitioning successful developments rapidly to the field.

Chapter 2-5. Addressing Technology Surprise

Today's rapidly changing world situation includes state and non-state adversaries with capabilities to inflict highly disruptive damage on U.S. interests and its way of life. In this environment, there is a critical need for the United States to rapidly and accurately assess and characterize the threats, determine options for effective counter-measures, and employ decisive action to mitigate the threat.

The emergence of overseas innovation, migration of R&D efforts to offshore sites, and the ubiquitous access to leading-edge technology makes detecting technological developments that have the potential for creating surprise a particularly challenging problem. The activity cycle for the Capability Assessment, Warning, and Response Office (CAWRO), recommended by the study team in Volume I of this report, and shown in Figure 2-10, outlines the approach to assess, warn, and respond to capability surprise.

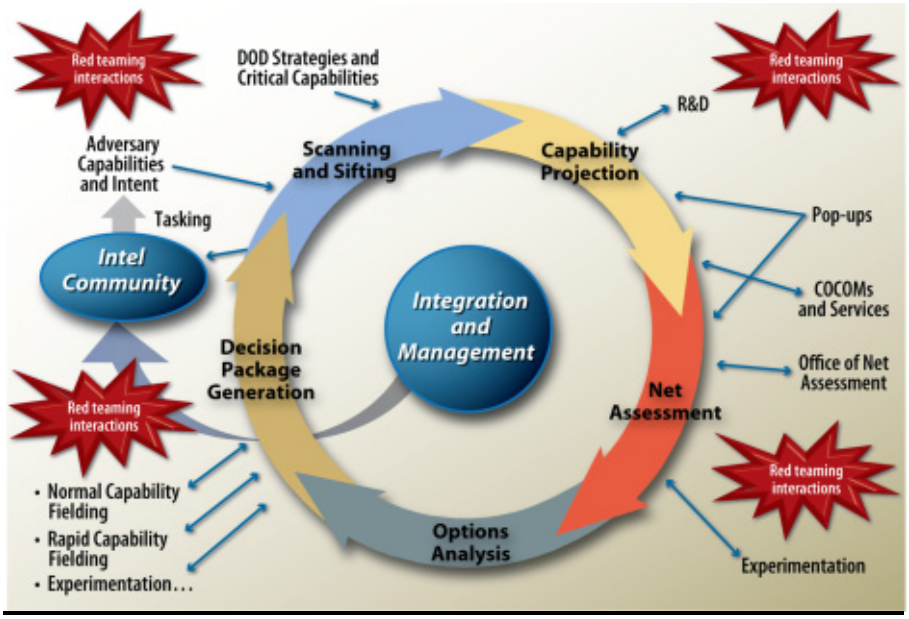


Figure 2-10. Surprise Management Cycle

In the framework for technology surprise (Figure 2-2) and the CAWRO cycle (Figure 2-10), the early focus is on collecting signatures, analyzing data, assessing threat potentials, and analyzing candidate responses. These elements, as described below, provide a technical framework to preemption and response.

Scanning and Sifting, Capability Projection

Monitoring and Detection. The processes needed to monitor foreign technical capabilities are an adaptation of techniques used in conventional dynamic threat monitoring, including:

- collecting data from all available sources
- combining those data into comprehensive assessments of foreign capabilities
- using those assessments to guide additional collections—including active measures that provoke additional signatures for exploitation

In this framework, the target signatures and scale differ significantly from that which our nation has grown used to over the past 50 years. Instead of a monolithic adversary, the United States faces a highly diverse set of related but uncoordinated technical projects. Instead of an international technical population somewhat less than that in the United States, our nation faces activities almost an order of magnitude larger.

U.S. intelligence collection and analysis tools simply do not scale to this domain. With a limited number of technical analysts, the United States must be creative, in at least three dimensions:

1. exploitation of new classes of signatures, especially those made available through the same expansion in global connectivity that supports international collaboration
2. imaginative use of emerging technologies to vastly increase the productivity of intelligence analysts, allowing them to cover the larger target set and absorb the vast amounts of new signature data potentially available

3. continuous adjustment of the areas of most intense observation, both within the analysis process, and through direction of collection efforts

All three dimensions fit into a "coarse-to-fine" paradigm, where all known activities are monitored at a course level (horizon scanning) and those efforts that are likely to create a significant threat are selected for greater attention (technology watch). The technology watch domains will frequently emerge and change, so their selection should not be permanently established in any formal organizational sense.

Exploit Novel Signatures of Technical Activities. In 2002, a seminal paper by Barabasi, et al., entitled "Evolution of the Social Network of Scientific Collaborations," opened the field of scientometric analysis.[28] Subsequent work has strengthened and adapted social network analysis models to identify emergent behavior of very weak networks.[29,30] These tools are routinely used today in the field of bibliometric analysis to identify the size and relative impact of research groups.[31]

This approach has resulted in horizon scanning and technology watch tools that are in use at the NGIC and the UK's Dstl. Horizon scanning requires data on a broad range of technical activities—broad in the geographical, scientific, and observational sense. To achieve this range, horizon scanning is targeted on the two signatures common to all areas: the people and institutions generating innovative technical ideas. These signatures provide pointers to identify innovative new concepts, emerging fields of endeavor, diverse funding arrangements, and dissemination mechanisms that connect the network.

---

28. A. L. Barabasi, H. Jeonga, Z. Nédaa, E. Ravasza, A. Schubert, and T. Vicsek, "Evolution of the social network of scientific collaborations ," *Physica A* 311, no. 3 (August 2002): 590–614.
29. Upadhye P. Rekha, V.L. Kalyane, Vijai Kumar, and E.R. Prakasan, "Scientometric analysis of synchronous references in the Physics Nobel lectures, 1981-1985: A pilot study," *Scientometrics* 61, no. 1 (September 2004): 55–68.
30. A.E. Cawkell and E. Garfield, "Assessing Einstein's impact on today's science by citation analysis," in *Einstein: The First Hundred Years*. M.Goldsmith, A. Mackay, and J. Woudhuysen, eds. (Pergamon Press: Oxford), 1980, pp. 31–40.
31. W. Koehler, et al., "A bibliometric analysis of select information science print and electronic journals in the 1990s," *Information Research*, 6, no.1 (2000).

The panel's recommendation in this area is straightforward: gather new signatures emitted by otherwise covert R&D activities, and use sophisticated automation to deal with the resulting huge volumes of data (Figure 2-11). Items in yellow describe the sources, process limitations, and products typical of the way things are done now; items in green convey the new elements that support expanded signature analysis. The backdrop portrays an example of the capability envisioned here: finding a website in China, then automatically extracting the entities, relationships, and key technical ideas reported therein.

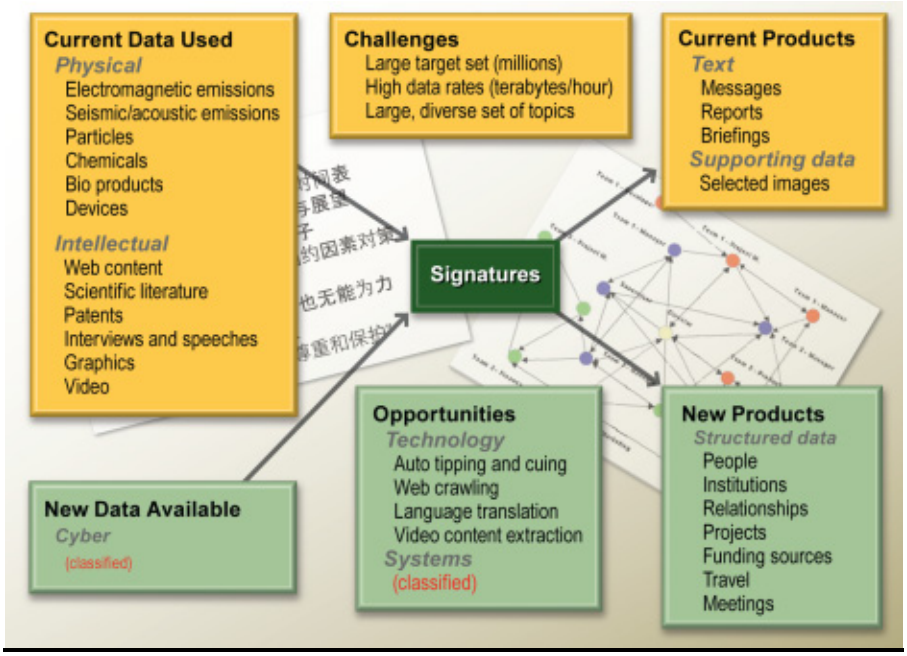


Figure 2-11. Expand coverage of indicators of foreign technical progress

The challenge of using horizon scanning tools at the scale required is finding weak signals in the enormous volume of open source data, much of which is now on-line. In 2003, the OECD estimated that over 600,000 articles appeared annually in the scientific literature. Manual exploitation of this volume of source data would be prohibitive. A comprehensive suite of automated exploitation tools, largely developed under DARPA sponsorship, has matured over the last decade to provide a basis for this approach. For example, these technologies continuously catalog web content, translate foreign languages to

English, extract entities and relationships from text data, convert speech to text, and generate alerts when specified linguistic patterns appear. These technologies produce machine-readable outputs (*e.g.* entity-relation data) that can support additional automation in downstream processes. Coverage gaps in traditional media can be closed by exploiting global connectivity to access additional cyber data. Data from these new sources can be processed in an automated fashion, without corresponding increases in staffing. Early research has captured salient content from the network and is beginning to explore the possibility of identifying emergent intent.

Continuously Track Technologists, Their Capabilities, and Their Relationships. Technology watch accumulates the material extracted from signatures, old or new, into comprehensive assessments of foreign technical capabilities—ideally before they surprise us. This process will never be fully automated, so it will be possible only in selected areas and will necessarily be limited by available staff.

Again, to maintain flexibility, we believe that the processes and tools should focus on the elements common to all technical development: people, their skills, and their relationships. Figure 2-12 summarizes the rationale behind this position.

Technology watch begins as a semi-automated process. It requires a focusing mechanism to select the areas with the most significant potential for surprise. Fortunately, the U.S. science and engineering community continues to build relationships with foreign technologists and their institutions, whether through academic collaboration or multinational business interests. As mentioned previously, universities and industry perform their own types of technology watch, albeit in domains tailored to their interests. DOD analysts should leverage, not duplicate, this work by building relationships with the domestic technology community.

Nonetheless, automation can help. Once the areas of interest have been selected, automated tools can mine the (machine-readable) data generated from signatures to augment, revise, confirm, or deny hypotheses about the state of foreign technology. Tools for social network analysis, link discovery, and various other forms of pattern analysis continue to mature and expand the domains of interest.

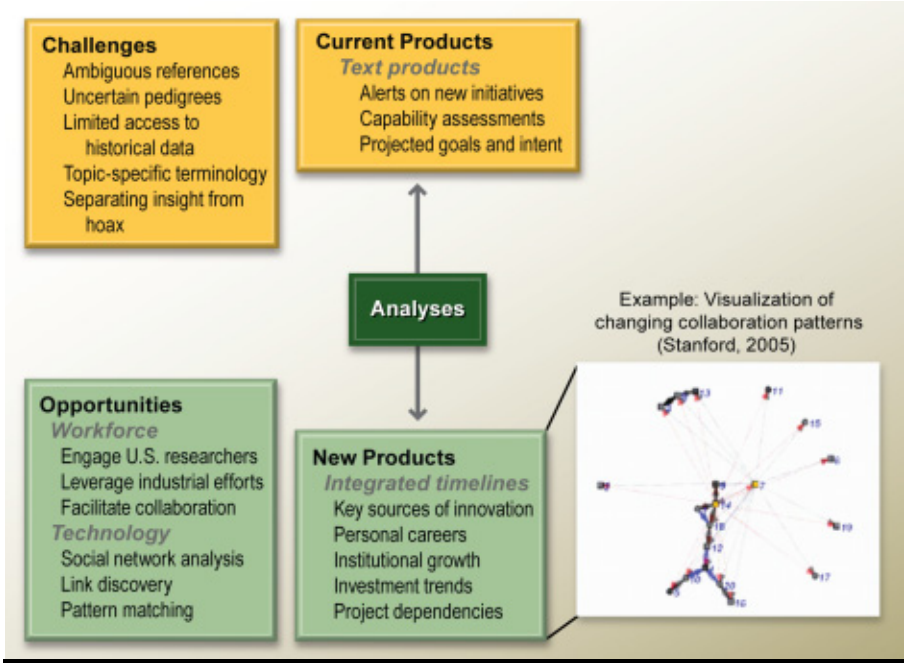


Figure 2-12. Improve timeliness and accuracy of analyses of foreign technologists and institutions working in selected technical domains

These tools also offer the potential for entirely new kinds of analysis products. In an era of constant institutional change through recruiting, mergers, acquisitions, divestments, joint ventures, and other novel business relationships, keeping track of the history of a specific technical initiative can be very difficult. Some of the aforementioned tools include creative visualization devices that allow one to quickly comprehend the history of the team affiliated with an initiative. By leveraging similar efforts in industry and academia, DOD will be able to operate with far fewer staff than would be required by a stand-alone organization. By using automated tools to associate signature data with specified technology watch topics, analysts will be able to construct assessments more rapidly and with greater detail.

Expand Access to Foreign Technologists. Influencing the process described thus far can be done in two ways. The United States can influence what other nations do, or influence what the nations or individual foreign technologists reveal. The most dramatic example of the former was the Israeli attack on the Osiris reactor in Baghdad in

1981—an event that set back that particular technical effort almost permanently. Diplomacy offers less dramatic mechanisms, such as the Nuclear Test Ban Treaty or the Chemical Weapons Convention.

In this section, though, we only address the second mechanism: creating new channels through which signature data can be obtained by taking actions that create open international forums where U.S. and foreign technologists are invited to discuss their research. Fundamentally, this involves opening and sustaining channels to foreign scientists and engineers (Figure 2-13).

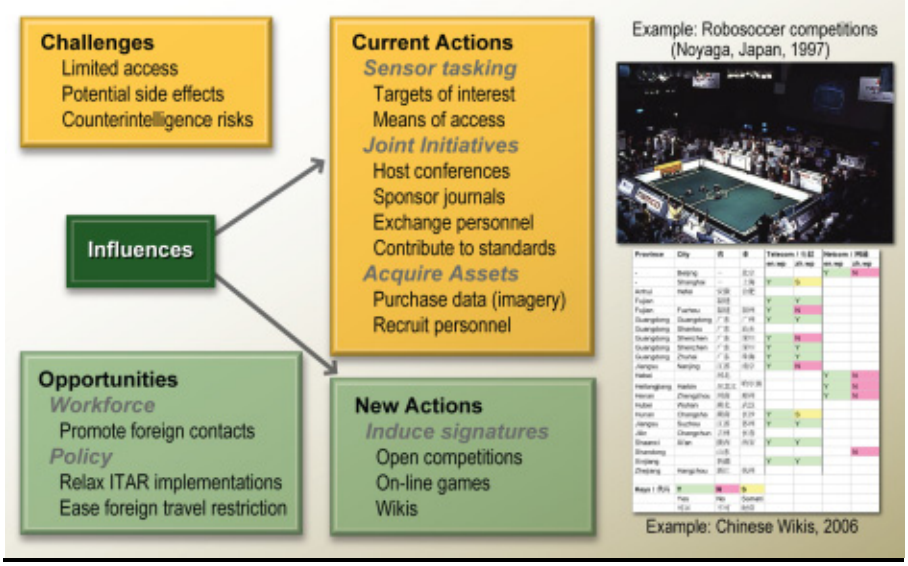


Figure 2-13. Expand access to foreign institutions and personnel; establish new forums for observation

Creating contacts with foreign technologists will always involve a trade between information obtained and information revealed. During the Cold War, when the United States had perceived technological advantage over the Soviets in terms of research and development, the United States could be quite protective. In today's global environment, where there is significant offshore technology development and the U.S. global technology lead is getting smaller, the balance needs to be different. Our nation has more to gain by being openly engaged in the international community, although technologies that afford the United States the element of surprise must continue to be protected.

Barriers established years ago to limit foreign contact now inhibit U.S. ability to observe offshore activities. Personnel with security clearances are required to report contacts with foreigners. Foreign travel by government employees is discouraged, yet personal contacts in industry often open many more doors in industry than do official government channels. International Traffic in Arms Regulations (ITAR), at least as interpreted by officials who monitor them, prohibit U.S. researchers from talking about topics and techniques that are common knowledge overseas. These regulatory processes need to be reviewed and amended to ensure that in today's world the benefits still outweigh the costs.

Another approach is to encourage foreign technologists to reveal themselves. International competitions, such as robosoccer, draw thousands of participants and reveal aspiring contributors to robotics technology. On-line games, especially those with complex technology-advancement elements, draw millions of players, particularly in east Asia. Wikis allow anyone to post information for the good of the community, including the United States (though China regulates these sites intermittently). DOD should at least observe these events and, following the example of the DARPA Grand Challenge, even sponsor them in areas of specific interest.

The payoff of these initiatives will be:

- increased visibility into foreign technical populations, through their involvement in open technical activities
- increased cost to opponents who desire to hide their activities, as they must close more channels opened by the actions taken by the United States to encourage an open dialog with foreign technologists

Taking a Deeper Dive. As a result of the scanning and sifting process, sometimes a new or emerging technology effort will be uncovered that warrants a more thorough capability projection.

Net Assessment and Options Analysis

Technology Red and Blue Teaming. As described earlier in this report, red and blue teaming play a key role in the net assessment and options analysis portion of the decision-making cycle. In general terms, the "red team" works from the adversary perspective to assess and highlight U.S. vulnerabilities, while the "blue team" operates as the United States to assess the country's capability against an adversary. Red and blue teams have long been used as tools by the management of both government and commercial enterprises. As detailed in the 2003 *Report of the Defense Science Board Task Force on the Role and Status of DOD Red Teaming Activities*, a number of long-standing red teams are a valuable part of the DOD, including the Air Force Red Team, Missile Defense Agency's Red Teams, the Navy SSBN Security Program, and the Army Red Team.

These red teams vary in their scope and depth, but have a number of characteristics in common, including, to varying degrees, top cover, robust interactions between red and blue, and the careful selection of a diverse (in experience and background) staff. The most important characteristic of successful red/blue teaming seems to be the creation of an environment that not only tolerates, but values criticism and failure for the sake of closing vulnerabilities, improving operations, and/or reprioritizing activities or investments. This is a difficult, but critical adjustment to current military culture in many areas.

There are a variety of types of red and blue teams. This panel report describes technology red/blue teaming. As shown in Figure 2-14, both the red and blue teams are focused by a particular threat-enabling technology. These teams have the capability to both mitigate and create surprise. (The process by which this is carried out and the composition of the red and blue teams are discussed in the following two sections.)

The red team identifies and prototypes new threats to U.S. military capability using knowledge about the adversary, the technology of interest, and knowledge of U.S. vulnerabilities. High priority new threat capabilities are passed to the blue team so they can begin to develop countermeasures or figure out how the same threat capabilities could be used against the adversary.

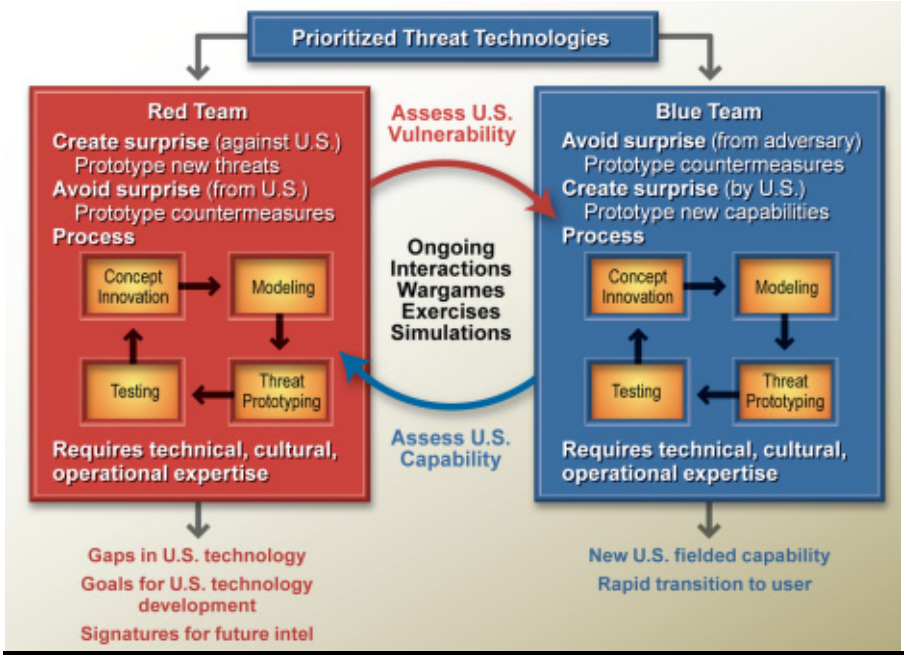


Figure 2-14. Technology Red/Blue Team Framework

Working in parallel, the blue team identifies new technologies that could be used against an adversary, either as a new capability or as a countermeasure. Valuable new technologies developed by the blue team should be transitioned to the user—facilitated by a streamlined process for transitioning a prototype to a fielded capability. These technologies should also be fed to the red team so that they can identify countermeasures to the proposed capability or determine how the new capability could be used against us.

Informal interactions between the red and blue teams should be ongoing, with regular formal interactions in the form of war gaming and exercises. These interactions can ensure that the threats and responses continue to evolve. In war games, the teams must be free to play "without a script" (i.e., use whatever capabilities they can think of) to stress the developed capabilities and highlight new vulnerabilities. A "hot wash" or "after action report" process should be in place to derive and archive lessons learned from the exercises.

Red/Blue Team Process. The processes employed by the red and blue teams to create and mitigate surprise are similar to each other, while the red/blue perspective (adversary or U.S., respectively) with which they are carried out differs. As shown in Figure 2-14, the common process often begins with concept innovation, which derives from a combination of knowledge of the technology, operations, and access to a motivating problem or vulnerability. The concept innovation results in a concept or concepts which are then modeled and analyzed to determine the feasibility of each and find the best potential solution. These steps require a combination of technical access, problem access, innovation tools, and modeling tools.

At this point, if the concept appears feasible and useful, a prototype is designed. Otherwise, the concepts may be modified or new concepts may be developed to better suit the problem. Prototyping demonstrates that the engineering is correct and proves the viability of producing the solution. The prototype can then be tested against the threat (United States or adversary) to determine operational impact and utility. A successful prototype can begin to be transitioned to the user community via a transition and fielding process (discussed in Volume 1 and in Part III of this volume). Testing results can also be used to validate modeling or inform additional solution concepts.

Formation of Technology Red and Blue Teams. Red/blue teams operate best as small groups. As a result, forming one overarching red and blue team that covers all potential threat technology areas is not desirable. Instead, the formation of these teams should occur in response to prioritized threat technologies. Once prioritized threat technologies have been identified, the United States should leverage existing, successful red/blue teams, if possible. If an appropriate group does not exist, a new red/blue capability should be formed. Forming these groups can be facilitated by knowing in advance where the domain expertise lies, as well as having a set of guidelines and/or processes for forming a new red/blue construct. These guidelines should include a combination of best practices from existing red teams.

The red and blue teams (which may be separate groups or combined in one place) should be similar in composition. The teams should be made up of technical and operational experts, who will help determine

operational utility of capabilities. Additionally, each team should have cultural experts, who can inform the teams as to how the other side (*i.e.*, the United States for the red team and the foreign adversary for the blue team) thinks and operates. They should also have access to the intelligence community.

The group of technologists should include a variety of backgrounds and areas of expertise. Focused technology watchers are able to identify the global innovations in the particular technology area. Technology horizon scanners are equally important in finding new advances in other technology areas, which may be coupled with the technology to create a new capability. These activities, along with cultural and operational expertise to provide context, will create new concept innovations. Scientists who specialize in modeling and analysis are critical to evaluating the utility and feasibility of new concepts. Finally, the team needs engineers who can design and build the initial prototypes. These teams must also be tied into relevant test sites or have the capability to do the testing.

Decision Options Generation

There is a need to institutionalize a process that ensures that decisions are made appropriately and promptly relative to a U.S. response to capability threats from adversaries. To accomplish this, this panel, along with the rest of this study team, recommends establishing a dedicated office, the CAWRO, which reports directly to the Secretary of Defense. This office will be the entity charged with sorting through the myriad of potential surprises and determining possible impact of these on U.S. defense capability. It will be the organization whose goal is to prevent or mitigate capability surprises with the charter to rapidly develop decision options for the Secretary. The CAWRO is envisioned as a small (100–200 professionals) office with broad technical, intelligence, and operational knowledge that can access all-source information. The CAWRO director should frequently meet with the Secretary to update him or her on changing futures. Appendix 2-B details the roles and operations of the CAWRO as perceived from the Technology Panel's perspective.

Evaluating and Reacting to Technology Surprise. The decision-making process turns on how well relevant information can be integrated and evaluated, applying appropriate criteria such as likelihood and consequence, to determine the proper course of action. Essential to this process are the following elements:

- **Sponsorship**. Technology surprise—both detecting and creating it—must be a high priority of the Secretary of Defense, who must allocate resources as well as personal time and attention to this subject. The Secretary must also reinforce the value of innovation and creativity with DOD.
- **Leadership**. A top executive in the Department must assume the responsibility for technology surprise. The scope of activities should expand beyond the traditional role of surprise prevention (recognizing that the United States will not lead in all areas and therefore surprise cannot be prevented in all cases), and should include:
  - gathering, integrating, and evaluating information from all relevant sources
  - issuing early warning/identification of technology surprise threats
  - reacting to these threats and taking steps to counter or mitigate them
  - serving as the primary DOD interface for this issue to other communities
- **Resources**. CAWRO should be allocated adequate resources for conducting experiments, exercising red teams, developing countermeasures, and other essential activities.
- **Cooperation and Communication**. To mature its ability to evaluate and react, it will be necessary for DOD to enlist a broad base of support and to communicate across a broad community the nature of various threats, their likelihood of occurrence, their consequences, possible actions to prevent or mitigate, and the uncertainty in assessing those factors.
- **Rapid Acquisition**. In response to certain potential surprises, the Secretary of Defense may decide that a rapid acquisition and

fielding program is required. (See discussion on rapid acquisition and fielding in Part III, Transition and Fielding, of this volume as well as in Volume 1 of this report.)

Finally, the community should develop a language and unifying concepts to promote understanding and broad engagement. For example, the climate change community has adopted guidance by which to consistently deal with uncertainties—guidance that includes a typology of uncertainty, calibrated language for levels of understanding and confidence levels, and a likelihood scale that correlates terminology with probability of occurrence. A number of communities have adopted a risk management approach (risk being defined as a product of four factors multiplied together: probability, threat (capability and intent), vulnerability, consequence) to assess relative importance and to make resource allocation decisions.

Sample Applications of the Recommended Process

To illustrate the application of the panel's recommendations to counter technology surprise, we investigated two potential surprise areas in some detail: biology and quantum computing. The remainder of this chapter provides an overview of these areas and how the principal recommendations for threat identification and decision-making apply.

Biological Surprise

Biological threats encompass not only infectious agents but also biomaterials having importance in medical and industrial applications. Medical applications can include the utilization of naturally occurring materials to compromise immune function and render host populations susceptible to minimally infectious organisms. Other aspects of physiology that can be affected include cognition, decision-making, and situation awareness. Biological agents that seriously modify or degrade these capabilities are currently available. Recent advances in biotechnology present new possibilities in the area of materials and energy. Biothreats do not recognize national or geographic boundaries, are relatively easy to produce, and require low economic investment.

For these reasons the ability to track biological anomalies will require collaboration with international agencies, and argues for monitoring collaboration networks of investigators, as discussed earlier in this part of the report.

Identify threat. In the case of infectious agents or toxins, a key concern is naturally occurring or genetically modified pathogens (bacteria, viruses, fungi, and toxins). Here, surveillance and cooperation by agencies such as the Centers for Disease Control and Prevention, the World Health Organization, and the Pan American Health Organization, as well as by normal information collection entities in the government, can provide early detection and identification of the threat agents. The identification of infectious agents involves characterization of genomic and proteomic markers that differentiate the threat agent from similar but non-pathogenic organisms. All geographic regions in the world have different levels of naturally occurring biological threat agents. To permit detection of anomalous levels or types of threat agent, it is necessary to establish databases of the normal distribution of such bioagents in geographical areas of interest. For this purpose the intelligence community, including the Defense Intelligence Agency, has ongoing activities. If there is an anomalous level or type of agent detected in a production facility, a restricted geographic location, or an area where forces are deployed, then a signature alert is given. Since disease emergence is a natural process, changes in level or type of threat agent may not be related to malevolent intent of an adversary, and the challenge will be to sort out natural from intentional outbreaks.

The above paragraph discusses detection of threat agents after the fact. To anticipate new threat capabilities in biological science or biotechnology, it will be important to track publication trends to spotlight reports of new agents, technologies, and applications of biological importance. Identification of new agents or materials that compromise neural function or host susceptibility to infectious agents should be one primary area of concern. Other applications may affect the stability of critical materiel or energy sources. All the technologies discussed in this paragraph are dual-use. Therefore a background level of legitimate investigation of pharmacological and electronic products based on biomaterials or biomimetics must be established. Research activities that span traditional discipline borders (*i.e.* biotechnology, nanotechnology,

and microelectronics) are of particular importance in the context of technology surprise.

Analyze impact. The degree of response to an anomaly or potential new threat capability will depend on an assessment of the potential negative impact on the U.S. population and/or blue and coalition forces. For example, the impact of a pathogen is a function of agent transmissibility, virulence, and weaponization potential. The impact estimate includes numbers of people affected, geographic distribution, economic loss, and effect on national stability. This analysis should include an assessment of countermeasures to the infectious agents (*e.g.*, National Pharmaceutical Stockpile and vaccine production capability).

The effects of anti-materiel biological agents on economic and infrastructure stability will require assessment by scientific and executive components of DOD and other government agencies. The effects of biological agents that impede or otherwise interfere with cognition, decision-making, and situation awareness on deployed blue forces or on U.S. nationals will also require such assessment.

Take action. For the most serious threats, an important part of the evaluation process will require red team/blue team exercises and simulations to determine the potential impact of an outbreak in the population or an attack on U.S. forces. Because the development of counters/therapies to biological agents may take some time, it is important to begin research as soon as a credible, potential threat is identified. Also, since the threat of retaliation may have a deterrent effect, techniques to trace the origin of an attack to its source is important to provide attribution capability. The difficulty of the attribution challenge cannot be underestimated.

Quantum Computing Surprise

The discoveries in 1994 by Peter Shor of two seminal quantum computing algorithms alerted the cryptographic community to a potential threat.[32] Shors' algorithms for factoring the discrete-logarithm problem,

32. P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (Washington, D.C.: IEEE Computer Society) 1994, pp. 124-134.

which would run in polynomial time on a quantum computer, represented threats to the essential underpinnings of public-key protocols. This in turn threatened the key-management infrastructures globally. Of course, a quantum computer did not exist at the time and still does not exist in 2008. However, the cryptographic designer does not have the luxury of sitting on the fence when faced with long-term threats, especially when those threats lie at the very heart of securing U.S. government and military communications.

Implementing a new key-management infrastructure is extremely costly in terms of time and money. A conscious decision was made by the National Security Agency (NSA) Cryptographic Research and Design Division (R21) to become a fast-follower in the area of quantum-computing algorithms. This area was viewed as an emerging branch of mathematics, not a place to lead, but certainly an area to fast-follow as crypto-mathematicians rely on many other areas, such as number theory, group theory, and algebraic coding theory.

Drawing on its world-leading experts in cryptography and cryptanalysis, NSA began a program in 1998 to take on the challenge of designing quantum-resistant public-key protocols. While unlikely to be leaders in the area of quantum computation, there was enough talent in this group to believe that a sufficiently high level of competence could be established to follow world developments, assess the potential of the new quantum paradigm, and ultimately present a picture that would inform the design environment. In 2000, a group of fifteen NSA crypto-mathematicians was formed to work full-time on coming up to speed on quantum computation. At the end of this start-up activity, many of these researchers returned to (or were recruited by) R21.

In 2001, R21 joined with the Army Research Office to fund promising research in quantum computing algorithms throughout the United States and Canada. Historically, R21 had not been a funding organization, but in order to maintain its leadership position in cryptographic design and to understand the threat, it was deemed necessary to cultivate relationships with world-class researchers in quantum algorithms. Effectively, the idea was to “stir the pot” and see what the real gunslingers could do. In this way, relationships have been established with the best quantum-computing algorithm research centers in North America and, indirectly,

with some of the best researchers worldwide. R21 and the Army Research Office conduct an annual Quantum Program Review, which all primary investigators are required to attend. Over 100 researchers attend the program review.

Parallel to the funding effort, the Institute for Defense Analysis (IDA)–Princeton and IDA–Bowie offered surge capability in the quantum research arena. A serious exchange with second parties also evolved, which included, among other things, a series of weeklong meetings (QUINCE) on the topic. To date these meetings have taken place in Cheltenham, England; Ottawa, Canada; and Canberra, Australia. QUINCE 2008, which expects to attract about 50 researchers, was held at IDA-Bowie, with invited speakers representing the R21-funded academic researchers on a day set aside for unclassified presentations.

R21 continually harvests results from both internal and external sources to inform its design environment. This approach has proven to be enormously effective. NSA successfully harnessed the expertise of crypto-mathematicians to produce a cadre of personnel knowledgeable in quantum-computing algorithms. This, of course, was done with the goal of maintaining NSA's pre-eminence in cryptographic design. And to do so, it is frequently necessary to fast-follow in one area in order to maintain leadership in another.

Chapter 2-6. Summary of Findings and Recommendations

Findings

As a result of its deliberations, the technology panel reached the following primary findings:

- Today, science and technology has become a global activity with rapid development of capabilities outside the United States. We as a nation can no longer assume that most technical advances will be initiated in the United States and rely on protecting our nation's technology edge. Adversaries will increasingly leverage technology to challenge the United States, often via military application of dual use technology created in the private sector. DOD does not have a strategy and process to identify and respond to rapid global innovation.
- Technology innovation requires the confluence of the technology itself, its application, who is applying it, and when it will or can be used.
- DOD and the intelligence community are having difficulty attracting and maintaining the technical skills to track and understand an exploding global technology landscape. The problem is both consistent funding and the attractiveness of career development/retention options. However, the U.S. research community is well positioned to understand the state of global basic research through open publications and peer channels and collaborations.
- The need for competitive advantage (proprietary knowledge) in new capabilities often drives technical innovation underground—whether new science or new applications of existing science.

Recommendations

The Technology Panel has four primary recommendations that are critical to improving the Department's ability to anticipate and respond to technology surprise. While the panel recognizes the importance of creating technology surprise, it was not a major focus of its study since we judge that DARPA currently does a good job in this arena.

RECOMMENDATION 1. ESTABLISH A DEDICATED CAPABILITY ASSESSMENT, WARNING, AND RESPONSE OFFICE.

DOD and the intelligence community should create a dedicated staff (the Capability Assessment, Warning, and Response Office) with a critical mass on par with similar activities in private sector multi-national firms (100 to 200 technical analysts) to conduct competitive analysis of emerging technology advances, to identify key players and highlight social networks of innovation, to target intelligence collection, and to project potential capability surprises and candidate responses. As described in Chapter 2-5 and Appendix 2-B, the CAWRO should consist of two directorates—Threat Assessment and Option Analysis—that interact extensively with the intelligence community, the military services, and the international technical community to scan for potential surprises and develop response options for action by the Secretary of Defense. The panel also recommends that, in addition to the staffing described above, CAWRO be supported with additional funding of $25 million, to build tools to filter massive amounts of data from all sources to produce technical indications and warnings.

RECOMMENDATION 2. ADVOCATE RED TEAMING AS A KEY ELEMENT OF THE CAWRO.

Establish a structured red teaming process that identifies potential technology-based surprises and their impact:

- Staff with a combination of technologists, operators, and intelligence analysts.
- Inform the CAWRO by means of an adversary perspective of weaknesses and strengths—both adversary and United States.

- Leverage knowledge of U.S. offensive capabilities.
- Exercise in war games that stress U.S. systems to their breaking point.
- Schedule activity on a regular basis.

RECOMMENDATION 3. STRENGTHEN DIRECTOR, DEFENSE RESEARCH AND ENGINEERING (DDR&E) ROLE AS DOD CHIEF TECHNOLOGY OFFICER.

The Secretary of Defense should strengthen the role of the DDR&E as the Department's Chief Technology Officer. Specifically, the Secretary should signal personal interest in the potential for technology surprise to negatively impact national security by directing the DDR&E to:

- Create a Defense Technology Strategy as part of the Quadrennial Defense Review that identifies: (1) critical technologies where the Department can and must maintain a leadership position (*e.g.*, emerging material sciences developments based on nano- and bio-technology, offensive cyber warfare, nuclear weapon design); and (2) global technologies where the Department must become a "fast follower" (*e.g.*, health and physical performance applications of bio-technology, cyber defense, information technology applications). The strategy must define an approach for the Department to become a "fast follower."
- Establish an advisory panel that uses outside experts in the national laboratories, academia, and industry to advise on global technology developments with the Secretary of Defense personally.
- On a quarterly basis, review the global technology landscape and its implications for national security with the Secretary of Defense personally.

RECOMMENDATION 4. INCREASE THE TECHNICAL DEPTH OF THE DOD WORKFORCE.

Take action to increase depth and scope of the DOD technical workforce, including:

- Implement incentives for technical development led by the DOD workforce.
- Expand the National Defense Education Act and use it as a recruiting and development tool to attract scientists and engineers in emerging fields into the DOD workforce.
- Ease restrictions on foreign travel and encourage participation in international technical conferences and symposia. Include counterintelligence sensitivity training prior to sending DOD staff to these conferences as a way to address concerns about information loss from a more open international technical dialog.
- Establish and maintain both informal and formal funded channels to obtain information from non-DOD sources (academia/industry/trade organizations).
- For critical areas, place DOD S&T researchers in university, laboratory, and industry facilities.

Appendix 2-A. Wicked Problems

One analytical framework that can help the Department of Defense anticipate and prepare for capability surprise deconstructs and examines "wicked problems," which are complex, multivariable, and have no set solutions. This appendix gives an overview of wicked problems, some guidelines on their analysis, suggested applications, and case studies.

Definition of a Wicked Problem

A "wicked problem" is a construct devised by academic theorists Horst Wittel and Melvin Webber (Wittel and Webber 1973). Wicked problems are highly complex, wide-ranging problems that have no definitive formulation, are substantially without precedent, and have no set solution (Table 2-A-1). They are frequently entwined in other problems and contain contradictory or incomplete data. Wicked problems involve many stakeholders with competing viewpoints and goals. Attempts to solve these problems impact other issues, and solutions can simultaneously contain positive and negative results. Solutions to wicked problems are themselves complex. There is frequently no one identifiable solution for the multivariate problems. The search for solutions never stops; every implemented solution has consequences for the other aspects of the problems, making measuring effectiveness difficult, if not impossible. The solutions sets are not finite and there is no well-described or well-defined protocol of permissible operations.

A wide range of problem solvers utilize the wicked problems construct as part of their analytical toolkit. Social scientists examine disparate issues such as the global war on terror or public health issues. Systems engineers utilize this construct when developing large enterprise level systems (Gharahedaghi 1999). The "wicked engineer" must be prepared for a cycle of continual surprise and unintended consequences. Successful solutions are not an end in itself because, having worked on the problem, the problem has changed. In essence "playing the game changes the game."

Table 2-A-1. Characteristics of Wicked Problems

1. **There is no definitive formulation of a wicked problem.** It's not possible to write a well-defined statement of the problem, as can be done with an ordinary problem.
2. **Wicked problems have no stopping rule.** You can tell when you've reached a solution with an ordinary problem. With a wicked problem, the search for solutions never stops.
3. **Solutions to wicked problems are not true or false, but good or bad.** Ordinary problems have solutions that can be objectively evaluated as right or wrong. Choosing a solution to a wicked problem is largely a matter of judgment.
4. **There is no immediate and no ultimate test of a solution to a wicked problem.** It's possible to determine right away if a solution to an ordinary problem is working. But solutions to wicked problems generate unexpected consequences over time, making it difficult to measure their effectiveness.
5. **Every solution to a wicked problem is a "one-shot" operation; because there is no opportunity to learn by trial and error, every attempt counts significantly.** Solutions to ordinary problems can be easily tried and abandoned. With wicked problems, every implemented solution has consequences that cannot be undone.
6. **Wicked problems do not have an exhaustively describable set of potential solution, nor is there a well-described set of permissible operations that may be incorporated into the plan**. Ordinary problems come with a limited set of potential solutions, by contrast.
7. **Every wicked problem is essentially unique.** An ordinary problem belongs to a class of similar problems that are all solved in the same way. A wicked problem is substantially without precedent; experience does not help you address it.
8. **Every wicked problem can be considered to be a symptom of another problem.** While an ordinary problem is self contained, a wicked problem is entwined with other problems. However, those problems don't have one root cause.
9. **The existence of a discrepancy representing a wicked problem can be explained in numerous ways.** A wicked problem involves many stakeholders, who all will have different ideas about what the problem really is and what its causes are.
10. **The planner has no right to be wrong.** Problem solvers dealing with a wicked Issue are held liable for the consequences of any actions they take, because those actions will have such a large impact and are hard to justify.

Strategic capability surprise is a specific type of wicked problem. In the context of national security, wicked problems are compounded not only by our nation's adversaries, but also by variables created by ourselves, our friends, and nature itself. Understanding the reality of the moment is hard enough in normal circumstances. But in the case of wicked problems, it should be expected that adversaries will employ deception, just as the United States will seek to deceive and become unpredictable to avoid being surprised. As Josh Kerbel states, "It's not rocket science, it's more complex" (Kerbel 2004).

Addressing Wicked Problems

Conventional linear thinking, the common analytical approach, will arrive at less than complete or comprehensive conclusions when dealing with capability surprise. In an analysis of cognitive bias with regard to China policy, Josh Kerbel lays out principles to counter linear bias and mind-set (Kerbel 2004). According to Kerbel, an organization should:

- Culturally embrace uncertainty
- Emphasize the understanding of possibilities, not prediction
- Utilize alternative scenarios/futures regularly as a methodological approach to problem-solving
- Emphasize the explanation of the assumptions, key variables, and signposts for each scenario
- Resist the temptation to minimize analytical uncertainty by eliminating caveats
- Try to avoid picking a single result in the face of significant uncertainty
- Recognize that language both reflects and reinforces bias/mind-set and consciously adopt more non-linear terminology and metaphors
- Require all involved in the analysis to take a course in linear/non-linear thinking and dynamics
- Make a concerted and serious effort to pursue the development of agent-based modeling, visualization, simulation and other advanced computer tools and techniques for exploring and explaining the dynamics of highly complex and non-linear systems

Application within the Department of Defense

In previous periods where "surprise" was considered unacceptable, the Department reacted with alacrity, speed, and commitment. During these times, the DOD had:

- Concerted, long-term, senior-level commitment
- Oversight and responsibility vested in the most senior operating authority
- Dedicated and protected resources
- A professional, sustained cadre of personnel augmented by rotational personnel from the operational, technical, and intelligence communities
- Unique security arrangements that created an extraordinary level of protection for the activities, while at the same time within the activity eliminating all barriers to cross access to the security disciplines of the participants
- Continuous measure/counter measure deliberation:
  - exhaustive effort to understand what the adversaries know about the United States and how they know it
  - identification of U.S. vulnerabilities, regardless of adversary knowledge, and a process to ameliorate those issues
  - analysis of the consequences of all U.S. capabilities being placed at the disposal of the adversaries
  - knowledge of adversary current and future capabilities, their implications for U.S. security and the value of incorporation of those capabilities into our systems, tactics, and policies

In examining and preventing capability surprise for the DOD today, three shifts in the early 21st century merit attention:

1. Technology and the operational application of capabilities move across borders at accelerated speed in the information age. A breakthrough new development is globally accessible within a greatly compressed time period.

2. Knowledge of U.S. systems, vulnerabilities, predispositions, and objectives is more accurate, readily available, and pervasive than at any previous time.
3. The number and diversity of potential adversaries have expanded dramatically. Where in the past only a small number of international forces could inflict serious harm on the country or its international interests, a large number of potential adversaries can now cause egregious damage to U.S. national security.

For many decades, the DOD has sustained an aggressive combination of technology, operations, and policy initiatives to keep the nation secure. These expanding threats and limited resources demand that the Department be managed with a combination of the best possible intelligence, the most aggressive technology programs, and inventive operational applications. There is benefit in an explicit methodology to highlight opportunities for interdiction and/or misdirection.

One option is to have a high-level, centralized organization be responsible for preventing or mitigating surprise, as recommended in the main body of this report. A central organization could ensure a reasonably exhaustive, capability-by-capability evaluation of the likelihood that an adversary will achieve a symmetric capability at parity with, or beyond our own; and the likelihood that an adversary can counter/deny us a critical capability. A central organization can have all the access required to understand present and future military capabilities while still ensuring the secrecy and sanctity of U.S. development and operation of these critical capabilities. An organization that stands above the individual capability developers and maintainers can bridge across them and consider alternative courses of action that might hedge a capability in one modality with a capability or basket of capabilities across other modalities. And, an organization so-placed can actually manage the hedging process.

Case Study in Wicked Problems in the Intelligence Community

The U.S. intelligence community must continually deal with nonlinear variables, their implications, and constant change. One focus has been attempting to predict trends and policies within the Chinese government and military. Three perennial wicked questions involve China's political stability, its evolving role on the world stage, and its military capabilities and force structure. According to the article by Kerbel, the intelligence community's major problem in predicting Chinese behavior has been the following:

- *Oversimplification*. The debate on granting China normal trade relations in the 1990s centered on economic issues. Policymakers did not take into account the security and human rights issues that could have further instructed the U.S. decision to drop tariffs.
- *Not realizing the inevitability of unintended consequences.* China's entry into the World Trade Organization is again not just an economic event, but will have social, political, and economic effects for years to come. This action could cause "rising unemployment and demands for political change, on one hand, and the assertion that the World Trade Organization (WTO) will lead to exactly the opposite: extension of the political status quo because WTO-spurred economic growth will give the current regime greater legitimacy."
- *Wicked problems cannot be repeated.* Comparing China to the USSR leads to false analogies for analysts.
- *Timing cannot be predicted due to unpredictable inputs and outputs*. The Kuomintang (KMT) ruled Taiwan for fifty years, navigating the island's balance as an independent entity with China's insistence that it was part of greater China. Though many had predicted political reordering through the years, it was not until 2000 that the KMT lost its majority rule to the People First Party.

Case Study in Wicked Problem Solving in the Private Sector

Successful publicly traded companies are examples of agile organizations that can successfully navigate wicked problems. In fact, many companies have found that the normal strategic planning processes don't prepare them to deal with the challenges of surprise and are adopting "wicked problem" approaches to these challenges. Because such companies seek to increase value for their shareholders and their shareholders traditionally give the companies' leadership great latitude for quick changes in strategy and execution, they are structurally better-positioned to tolerate greater risks and apply creative, nonlinear, open-ended solutions to their wicked problems. Shareholders, via their board proxies, can quickly punish poor decisions and wrong turns in this process via changes in leadership and demands for immediate strategy changes. Wal-Mart offers an example of a wicked problem and two approaches that it took (Camillus 2008).

For almost fifty years, Wal-Mart has been enormously successful at increasing market share via low-cost sourcing and using loss-leaders in their merchandise inventory to eliminate competitors (at which time, they can raise the prices to market level). However, Wal-Mart's wicked problem is that they have saturated their target market, yet must continue to show their shareholders ever increasing value. In addition, all their movements affect differing stakeholders, including employees, trade unions, investors, creditors, suppliers, governments, and others, sometimes creating their own wicked problems (law suits and negative publicity about human resource abuses are recent examples). From the myriad of options available to address the wicked problem of shareholder growth in an almost fully saturated market, two examples emerge.

The first example of wicked problem-solving is to try to sell different products in the existing American market. Since Wal-Mart has saturated the suburban and rural markets with low-cost items, it has attempted to modify its value proposition by stocking some upscale products and developing a brand persona that warrants higher prices. By taking this tactic, Wal-Mart is taking the strategy of one of its main competitors, Costco, which regularly stocks mid to upscale items in a discount setting. Initial indications are that this strategy is failing

(Barbaro 2007). As with many attempted answers to wicked problems, Wal-Mart could not have anticipated the unintended consequences, namely that consumers devalued the upscale items and viewed them as cheap because they were in the Wal-Mart setting. Wal-Mart has now pulled back on stocking upscale items and is pursuing the higher price-point strategy via its introduction of organic foods.

Second, as part of a greater strategy to expand internationally, Wal-Mart has found a way to enter into India, which has particularly wicked, market-entry problems. India possesses laws that prohibit foreign companies from operating multi-brand retail outlets in the country. Wal-Mart responded by developing cash and carry wholesale stores for local retailers in a joint venture with Bharti Enterprises, an Indian telecommunications company. Characteristic of the wicked problem, a number of other wicked problems arise from this strategy: Wal-Mart must now work with the Indian government and within the Indian consumer products sector to build its supply chain. Additionally, if and when India's laws change, Wal-Mart will have to compete with the retailers that it supplies. These and other problems typify a business's challenges when confronted by non-linear strategic issues.

This cursory look at a business example can be replicated many times in the worlds of military, economic, political or operational capabilities. Wal-Mart's continually shifting approaches to its wicked problems exemplifies any organization's attempt to address nonlinear problems.

Summary

Wicked problems will characterize more and more of DOD's future challenges. This appendix has attempted to introduce the reader to the nature of such problems. There is a growing discipline of scientific investigation and management application in this area that DOD should become more aware of and begin to participant in. The inter-dependencies, complexities, and non-linear behavior of the modern world require something beyond the traditional approaches that were effective in a simpler time.

Works Cited

Barbaro, Michael. *International Herald Tribune*. March 2, 2007. http://www.iht.com/articles/2007/03/01/business/walmart.php (accessed August 30, 2008).

Camillus, John. "Strategy as a Wicked Problem." *Harvard Business Review*, May 2008.

Gharahedaghi, Jamshid. *Systems Thinking—Managing Chaos and Complexity: A Platform for Designing Business Architecture.* Burlington: Butterworth Heinemann, 1999.

Kerbel, Josh. "Thinking Straight: Cognitive Bias in the US Debate Over China." *Studies in Intelligence*, 2004.

Appendix 2-B. Roles and Operations of the CAWRO

The CAWRO should have two directorates, Threat Assessment and Options Analysis, each led by a deputy director. The deputy director of the Threat Assessment division should be drawn from the intelligence community. This group receives S&T intelligence signatures and cross-correlates this intelligence with key indicators (*i.e.*, technology application, potential target, actor, and timing factors). The CAWRO validates, verifies, and characterizes the threat. This systemic approach to threat analysis results in a statement of vulnerability to U.S. interests of the threat.

The second directorate, Options Analysis, is headed by a deputy with a military background. This division's function is to determine the potential impact of the threat, an assessment of the probability of the threat occurring, and the priority of the threat relative to other threats. With the use of red teaming, modeling, war games, and other tools, this group will define the range of actionable options to reduce the threat's impact and/or probability of occurring for presentation to the decision-makers. The Secretary of Defense, or his designee, will lead and make the necessary decision for the action to be taken.

In essence, the **Decision Cycle** proposed is a quantifiable process to flow requisite information to the nation's decision-makers for action. There are three key steps in this decision cycle: (1) Threat Assessment, (2) Option Analysis, and (3) Deciding. Input for this decision-making cycle is signatures analysis from the S&T intelligence community to the threat assessment step. The response taken is the output of the "deciding" step. Output of the threat assessment step is a formal statement of technological vulnerability provided to the option analysis team. The option analysis step provides options to mitigate or resolve U.S. vulnerabilities. Options provided include a full range of courses of action, from military intervention, to démarche, to the development of new technological countermeasures for the decision team's consideration. In the final step, "deciding," senior leadership selects, directs, and employs the appropriate response to mitigate the impact of an emerging technological disruption.

Whether the disruptive technology is from friend or foe, the decision cycle will help mitigate the effects of a disruptive technology.

To determine technological threats, the aggregate of five factors provides the basis of an indication of a potential threat in the threat assessment step. Technology assessment alone is not sufficient, as the technology used for surprise can be either new or commercially off-the-shelf. While technology horizon scanning and other methods are critical in determining new technology developments by adversaries (or available to them), it is not an indicator of a threat. The other factors taken together help determine whether or not an immediate threat exists. Necessary information includes identification of the actor(s) with the technology, whether they are a lone actor or a nation state, and what their intent is or might be. How the technology can be applied in novel ways must be assessed as well as whether or not the actor wants attribution.

Input to the **Threat Assessment** step is a signatures report that contains indications and warning of a possible threat to U.S. interests in the form of disruptive technology. In the threat assessment step, signature data are analyzed and evaluated to determine if in fact a threat exists and, if it does exist, the threat is characterized. To characterize the threat, information is synthesized, evaluated, and collated into five key areas. In this step, a determination is made as to magnitude of the threat and a formal statement of vulnerability (SOV) articulates the level of the threat (*i.e.*, high, medium, low, or no threat). The SOV details the impact to the United States (*e.g.*, infrastructure, biological, nuclear, or communication systems). However, the threat assessment step alone is not sufficient. The SOV is merely the input to the **Option Analysis** step in the three step decision process cycle.

Delivered to the Options Analysis process, the SOV provides the basis for generating option packages. The short-, mid-, and long-range option packages contain subcategories that have both resource constrained and unconstrained options. A critical part of option analysis is red teaming, which looks at not only U.S. vulnerabilities, but also options for mitigation of these vulnerabilities. Options Analysis must also quantify the probability of the threat occurring based on the readiness of the adversary and the adversary's goals. An assessment must be made to determine the reliability of the data being used for analysis. The threat's potential impact on U.S. interests and way of life,

including cost, where, and on whom, must be factored into the options analysis. With all these data, prevention options must be developed, considering costs, timing, global impact, and resource readiness. The output of the option analysis is presented to the **Decision Team**, led by the Secretary of Defense.

Decisions by the Secretary of Defense will range from initiating a normal acquisition and fielding program; to rapid development, acquisition, and fielding; to training and operational adaption; to proactive measures. The decision step must include iteration among the group, as well as with expert "outsiders." Iteration within the group as well as others' inputs will lead to the best decision. Part of the decision needs to be the level of response to the threat, including the priority of this action versus other activities ongoing or in planning, the political ramifications of taking action, and the decision of when to respond. Communicating the decision to all appropriate parties is the final element to taking action.

Each of the three key steps (threat assessment, option analysis, and deciding) and the elements within each of these steps, need to be quantified. Qualitative assessments are not sufficient for adequate analysis. In addition, each step must be led by a predetermined organization and specific individuals who will lead multidisciplinary teams and encourage iteration for the most innovative conclusions.

The Director, Defense Research and Engineering (DDR&E) is a key resource for the CAWRO and should be allocated adequate resources for sponsoring experiments, developing countermeasures, and other essential activities. To mature the CAWRO's ability to evaluate and react, it will be necessary for DOD to enlist a broad base of support and to communicate across a broad community on a variety of topics including the nature of various threats, their likelihood of occurrence, their consequences, possible actions to prevent or mitigate, and the uncertainty in assessing those factors. The DDR&E should enlist the support of important partners such as other government agencies, academia, national laboratories, industry, and allies. Examples include the Technical Support Working Group, the National Science and Technology Council, and the Advisory Group on Electron Devices. The community should develop a language and unifying concepts to promote understanding and broad engagement.

Part Three.
Transition and
Fielding Surprise

Chapter 3-1. Transition and Fielding Surprise: Why Worry?

This report, prepared by the Transition and Fielding Panel of the Defense Science Board 2008 Summer Study on Capability Surprise, provides detail concerning surprise that results from unexpected adversary transition and fielding activities. Transition and fielding is the ability to move from ideas or concepts to fielded capability sufficient to create operational, strategic, or existential successes. Effective transition and fielding is critical to successfully contending with capability surprise when it is occurs.

Adversaries can deploy a concept, product, or system in several ways that can surprise the United States and pose a potential or real threat to U.S. interests, including:

- capabilities the United States did not know the adversary possessed
- capabilities the adversary created based on known subcomponents or pathways, but combined in a novel way or employed with timing and targeting that it is surprising
- capabilities the United States knew the adversary possessed but did not expect to be used, or used in a given setting

If the United States has not anticipated or adequately prepared for any or all of these approaches, they may be used to harm or threaten U.S. interests, missions, goals, or resources. When faced with such situations, the United States must act quickly to mitigate or limit potential damage, or it may face the potential of the threat cascading from the immediate surprise to a much larger concern that can grow beyond easy containment or control.

Two major aspects are involved when dealing with and/or mitigating transition and fielding capability surprise:

- **Anticipation:** detecting transition and fielding activities of others planning to surprise the United States.

- **Response:** speeding introduction of new or adapted capabilities to counter adversary surprises, including materiel, training, doctrine, and operational concepts.

Both aspects of addressing transitioning and fielding surprise can involve the full spectrum of capability conception, development, testing, production (if materiel), and fielding.

The threat of surprise is higher than ever before. The context for assuring national security is extraordinarily complex today, and the likelihood of transition and fielding surprise has increased substantially over the past several decades. A convergence of many forces is creating a uniquely challenging security context for the United States. These forces include the political dynamics of nation state changes since the end of the Cold War, the rise of radical Islam, the massive globalization of economics and communications, and shifting economic power towards rising states such as China and India. In addition, civilian vulnerability is higher while the global reach of adversary capabilities is greater and can be cheaply amplified. Table 3-1 outlines some of the current conditions that have resulted from these forces and created a higher potential for surprise.

Given this elevated threat to the nation, the stark differences in how the United States and its adversaries are able to transition and field new capabilities should be of particular concern:

- U.S. system and product capabilities are typically developed and produced within the Department of Defense (DOD) acquisition system, which is much slower than the rapid pace with which adversaries piece together components to create capability. Further, exposure of DOD system vulnerabilities during the system development cycle, when they can be more readily eliminated or ameliorated, is typically discouraged.

Table 3-1. High Impact Surprise Conditions Against the United States

Vulnerabilities	Motivated Adversaries	Enabled Adversary Functionality	Adversary Pathways
Self-inhibiting, Restrictive Values • "High value" of life • Human rules of engagement • Protection of individual privacy **Physical Fragility, Non-Resilience** • Human and asset concentration (urbanization) • Single point failure modes in infrastructure • Lack of self-sufficiency, interdependency, outsourcing, foreign supplies/products • Low excess capacity margin throughout economy • "Just-in-time" logistics; small inventories • Dependency on small numbers of expensive long-lead military assets **Intrusive Visibility, Penetrability** • Large diaspora 5th column • Globalization (international commercial intercourse) • Military and government family easy to identify	**Traditional (subject to retribution, sanctions, deterrence, and focused intelligence)** • Rogue state-based forces • Coalition of alienated states • Emerging technological and economic peers • Static exploitation of asymmetric techniques **Non-traditional (immune to retribution, sanctions, and deterrence)** • The "power of one" or a few as innovator or integrator • Transnational distributed terrorist networks • Rogue-state-sponsored organizations • Suicidal, martyrdom ethos • Anonymity or uncertainty of attribution of the perpetrator	**Worldwide access**	
		• Ubiquitous command, control, communications, and intelligence open to all	• Internet • Cell phones • Global Positioning System • Satellite mapping
		• Leveragable global reach without investment	• Cyber/information warfare • Receptive, exploitable media • Rapid, inexpensive global civil transport
		Weapon Access, Financing and Support	
		• Readily accessible, assembled, or manufacturable high-impact weapons	• Precision weapons • Improvised weapons • Weapons of mass destruction • Disruption of private sector infrastructure
		• Easy, substantial, covert financing	• Drug and oil funding
		Education and Technology Availability	
		• Rising worldwide education	• Un-retained or alienated Western-educated foreign students
		• Worldwide access to technology know-how, materials, and manufacturing facilities	• Knowledge openly available on the Internet • Private industry outsourcing/globalization • Ineffective export controls

- Adversaries who develop more complex capabilities aimed at U.S. security vulnerabilities may do so through means the United States would not use. Adversaries may not be governed by the same legal or ethical constraints that limit the United States. They may be less concerned with high or consistent levels of system/product performance, with safety, or with testing—all matters that govern U.S. acquisition. There is also often an asymmetric view of success—that is, traditional concepts of kill probability, leakage rates, collateral damage, and related factors are often viewed very differently by potential adversaries.
- Some adversaries target DOD or other U.S. government-developed technology for application in their transition and fielding capabilities to exploit U.S. vulnerabilities. They can achieve a cost and tactical advantage by avoiding technology development. It may not matter if they have only partial, incomplete, or less than fully functioning variants of U.S. capabilities, as long as they can effectively deploy them against our nation. Night vision capabilities are an example of such exploitation.
- Some adversary surprises require almost no transition and fielding effort because they are based on exploitation of widely available commercial capabilities or capabilities obtained from the global arms markets to target U.S. vulnerabilities.

The nature of transition and fielding surprise requires a response approach different from the mainstream DOD capability development process. Decisions to respond to transition and fielding surprise are often undertaken in periods of conflict, war, or extreme stress. When there is an urgent need, and particularly if military success and lives are being threatened, the military chain of command and DOD civilian hierarchy will likely be engaged quickly, and then at an increasingly (if not immediately) high level. Cases examined by this panel (discussed in the next chapter) point to an ongoing escalation of leadership involvement as the effects of surprises grew or became clearer, particularly once reported in the media. A lack of pre-surprise, scenario-based planning typically created the conditions for over-reaction. Rapidly increasing leadership involvement tended to coincide with the surprise

snowballing out of control, due to either inadequate responses provided too slowly or an inability at various decision points for leaders to see the full context and potential consequences. These decision shortfalls resulted in escalating problems.

Despite what were surely the best intentions and efforts from the military units up to the most senior leaders, the cases examined show that decisions and resulting actions were often:

- *inconsistent*—varying directions depending on the information assessed by decision-makers
- *incomplete*—possibly not addressing the full picture (*e.g.*, in the case of improvised explosive devices (IEDs), sequentially up-armoring, then trying to defeat the IED triggering, then fielding the Mine Resistant Ambush Protected (MRAP) vehicle, and then attacking the support network)
- *stopped short at some decision level*—the transition and fielding surprise consequences could be severe, but it was not yet clear

It is not that DOD lacks a clear chain of command or that leaders do not engage. Cases suggest that the military, at the operational level, is highly adept at dealing with tactical surprise quickly with the means at hand. But the potential threat posed by transition and fielding surprise is different in nature. In the cases examined, the transition and fielding surprises often first appeared to be a tactical issue, but in reality forebode a more strategic problem, so that normal mechanisms were employed initially to address the problem. DOD is not well-equipped to identify, prioritize, handle, and track these transition and fielding surprises systematically. The Department has developed requirements and acquisition systems that generally produce excellent weapon systems. Interfaces between users and acquisition communities have been created to provide orderly and disciplined inputs and responses. Yet these processes are also slow and complex, and contain many real and perceived checks, balances, approvals, and reviews that draw out reaction time.

The potential threat posed by transition and fielding surprise is different in that the need to respond is often immediate. DOD has created many urgent needs processes and rapid reaction programs, but the decisions about important transition and fielding surprises and today's

small but urgent needs from the field often end up in the same DOD action and decision flow. In today's DOD decision flows, decision visibility and accountability may be adequate to solve a near-term fielding issue, but could be lacking for a surprise with the potential for strategic damage (or worse). Further, the decisions for large, but less certain transition and fielding threats may not be made at all, as they may be anticipatory and fall outside the criteria for DOD's formal urgent needs processes or outside the clear responsibility of a specific DOD organization.

Chapter 3-2. How DOD has Dealt with Transition and Fielding Surprise: Case Studies

An understanding of DOD's ability today to address transition and fielding surprise was informed by interviews conducted with representatives of industry, government, and the intelligence community, as well as by review of relevant documents and studies. Numerous diverse examples of transition and fielding surprise activities within DOD were included in the panel's assessment. Three case studies were selected for a closer examination of DOD processes and experiences.

Examples examined in this study included both instances in which adversaries used transition and fielding capabilities to surprise the United States, as well as those in which the United States used transition and fielding capabilities to surprise adversaries. The examples reviewed ranged from cases where the United States surprised adversaries by inserting sophisticated capabilities developed over time and applied in weapons systems, such as in the case of stealth, to instances where the United States surprised itself by forgetting lessons learned from technology demonstration projects.

In addition the panel examined the Competitive Strategy—a large-scale U.S. strategic initiative, which was a contextual framework for U.S. assessments and actions vis-à-vis the former Soviet Union throughout the Cold War. Focused assessment within the Competitive Strategy framework provided an umbrella under which the United States developed several important surprise capabilities during the Cold War period, including the Strategic Defense Initiative and Assault Breaker.

For each case, the panel examined how transition and fielding capability surprise played out in both offensive and defensive scenarios, different technologies, organizations, and historic periods. Each had lessons to teach (such as unique software management issues). The three chosen for more in-depth assessment were most relevant to today's environment and exemplified common issues.

These surprise cases were reviewed for the entire surprise "life cycle," including the root causes of the surprise; how the surprise affected not only military, but public and institutional reactions; DOD's organizational, material development, production, and deployment responses; and if/how DOD garnered or acted upon lessons learned. For example, the first case on Scud attacks during Operation Desert Shield illustrates the dramatic impact of public perception on military and administration focus and reactions.

In a second case, a review of the IED response in Iraq, the approach included interviews with both former and current representatives from the Joint Improvised Explosive Device Defeat Organization (JIEDDO), the MRAP vehicles program office, and major firms supporting the MRAP program. Other inputs included relevant documents as well as input from additional firms supporting MRAP, the Office of the Deputy Under Secretary of Defense for Industrial Policy (ODUSD (IP)) on its industrial response lessons learned concept, and a White House Fellow assessing the MRAP case.

The third case is that of precision GPS (Global Positioning System), where the initial surprise led to others. At first, DOD was able to exert surprise in many exploitations of precision (*e.g.*, precision missile targeting). However, DOD has, over time, also been "surprised" by this capability, as the GPS domain has extended into a civilian capability. As a result of this shift, DOD has lost control over GPS use and system policy—an unanticipated surprise.

These case study reviews, by necessity of time, could not be fully comprehensive. However, examining and evaluating these case studies provided insight into the dimensions of DOD's response to and preparation (or lack thereof) for surprise.

Each of the three cases is described more fully in the sections below—examining causes, responses, institutional reactions, and overall lessons—followed by a summary of the lessons learned from the three cases (Table 3-2).

Case 1. Scud Attacks, 1990–1991 Persian Gulf War

Cause

At some time during Operation Desert Shield—the six-month period preceding Operation Desert Storm—Saddam Hussein decided to use Scud missile attacks to break the international coalition assembled by President George H. W. Bush. In particular, Hussein used Scud attacks to try to link the Arab-Israel conflict to the coalition's effort to force Iraq to abandon its conquest and occupation of Kuwait. Iraq's extended-range Scuds were of little military value; they were inaccurate and carried small conventional or inert payloads. However, as Saddam Hussein predicted, the Scuds had great strategic value. Then-Lt. Gen. Charles A. Horner noted in 1993, "I have never seen anything like the terror that was induced on the civilian populace of Tel Aviv and Riyadh from the Scud bombing."[33]

With hindsight, the evidence suggests that U.S. military commanders, intelligence analysts, and air planners were deeply surprised by the impact of the Scuds on public opinion in the attacked areas, particularly Israel.[34] The U.S. Air Force expected that destroying ballistic missile production and infrastructure would suppress missile launches during the war. However, this strategy proved to be ineffective because the Iraqis decided to rely on mobile launchers, enhanced by decoys and deception, and on using existing inventories. Most of Iraq's mobile Scud force dispersed from central bases by the end of August 1990 and remaining production was effectively concealed.

---

33. Charles A. Horner, "Offensive Air Operations: Lessons for the Future," *RUSI Journal* (December 1993), p. 22; Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report* (Washington, D.C.: United States Government Printing Office, 1993), pp. 83–90; Mark D. Mandeles, Thomas C. Hone, and Sanford S. Terry, *Managing 'Command and Control' in the Persian Gulf War* (Westport, Conn.: Praeger, 1996), pp. 70–80.

34. Michael R. Gordon and Bernard E. Trainor, *The Generals' War* (Boston: Little, Brown, & Co., 1994), pp. 228–229.

Response

The U.S. employed offensive and defensive means to counter the Iraqi use of Scud attacks. As a defensive effort, the U.S. provided Saudi Arabia and, shortly after the initial Scud attacks, Israel with Patriot missile defenses and communications links that increased the warning time of Scud launches. At the time of the attacks, Patriot was in the process of undergoing an upgrade with a new missile variant, PAC-2, that could engage tactical ballistic missiles. Only two prototypes of this configuration, surplus assets from the test program, were initially available during Desert Shield. As soon as the attacks started, it became apparent that modifications to the fusing and lethality functions of the existing missiles were needed.

The Army's Patriot Program Office and the contractor, Raytheon, began a crash effort to upgrade existing missiles. Patriot batteries in Israel and Saudi Arabia used the fielded missiles to conduct engagements of inbound Scuds. Those engagements, widely covered on television, reassured the civilian population of Israel and bought political breathing room by allowing the Israeli government to refrain from attacking Iraq. Offensively, on the first day of the air campaign, the U.S. attacked Iraqi fixed launch sites, production facilities, mobile Scuds, Scud hiding places, and communications nodes. As Iraq continued to launch Scuds, the U.S. increased its effort by assigning special operations forces to search the Western desert for mobile Scuds and their launchers, and by dedicating aircraft capable of firing precision-guided munitions to the Scud hunt.

Institutional Reaction

The Scud attacks generated some civil-military "friction," and diverted attention of senior civilian and military leaders to unanticipated, but urgent tasks. Senior civilian leaders were unhappy with U.S. Central Command's (CENTCOM) lack of understanding of the strategic implications of Scud attacks, as well as CENTCOM's conduct of tactical operations to eliminate the missile threat. Senior CENTCOM leaders, under intense pressure to end the Scud attacks, devoted a great deal of attention to reviewing and managing the Scud hunt. Their military plans became increasingly *ad hoc* as the Scud launches

continued. As a result, CENTCOM leaders devoted less attention to planning, guiding, and reviewing other pressing operational and strategic military tasks. Civilian leaders, too, were distracted by the diplomatic and political tasks of reassuring Israeli leaders—to prevent them from attacking Iraq—and of placating Arab leaders worried about the political and cultural implications of an implicit alliance with Israel against another Arab and Muslim state.

Overall Lessons

The existence of the Scud threat was well understood prior to Operations Desert Shield and Desert Storm, including knowledge that the range of the existing Scuds had been increased, that the modifications were poorly done, and that consequently the missiles had a tendency to break up in flight—all of which made effective defense more difficult. But Saddam Hussein's use of ballistic missiles against Israel and the political effect it would have were not anticipated. The U.S. response, even though somewhat limited in effectiveness, was enough to prevent Israel from striking Iraq, as Saddam had desired. However, had the Patriots not appeared to be effective, or had Saddam decided to use chemical warheads, the result could have been very different.

The Air Force also overestimated its own ability to neutralize the Scud threat, partly because it did not anticipate Saddam's course of action, and partly because it overestimated its own ability to find and kill Scuds and their support infrastructure. The lack of geopolitical perspective, failure to think creatively about threat courses of action, and lack of understanding of organic capabilities all contributed to the Scud surprise. Had these errors in judgment not occurred, a Patriot upgrade and other measures to negate the Scuds could have been undertaken earlier, and the risk posed by this threat significantly mitigated. The experience also demonstrated that when an urgent wartime need exists, the acquisition system has the ability to respond, albeit only under enormous pressure: two Patriot modifications were designed, tested, and fielded in weeks rather than years.

Case 2. Improvised Explosive Device Defeat in the Aftermath of Operation Iraqi Freedom

Cause

The invasion of Iraq in Operation Iraqi Freedom rapidly succeeded in the initial take down of organized resistance and the removal of Saddam Hussein, but did not succeed in establishing a secure environment among the many factions within the country. Saddam had dispersed massive munitions caches around the country. DOD leadership's decision to use a lean force and emphasis on speed to reach Baghdad led to the circumvention—rather than containment—of Iraqi munitions. Hence, vast quantities of munitions were available to Iraqi *fedayeen* and insurgents. Consequently, from the opening days of the war, U.S. troops confronted human-borne suicide and car bombs, roadside bombs (IEDs), foreign *jihadis*, and ambushes.

Response

Army and Marine commanders used existing tactics, techniques, and procedures to deal with Iraqi irregular forces. These early responses also reflected Service culture and training. In response to a detonated IED, soldiers and Marines dismounted their vehicles and sought to capture or kill the bomb commanders with limited success. As experience accumulated, tactical unit commanders jury-rigged *ad hoc* technical solutions (*e.g.*, jammers or added armor to vehicles). U.S. troops seeking to adapt to Iraqi insurgent tactics also employed informal arrangements—for example, asking family members in the United States to buy and send equipment.

The insurgents also responded to U.S. tactical adaptations. The hostile Iraqis (and their foreign supporters operating out of safe havens in other countries) observed and diagnosed U.S. tactics, jammers, and other technical means, and altered bomb design and components. Some U.S. military and civilian observers noted that the insurgent response cycle was far faster than that of the United States. Media reports raised the political urgency of the IEDs, and highlighted the tactical impact of IEDs, which accounted for more than half of all casualties.

Institutional Reaction

Higher military and civilian organizational echelons initially used stepped-up versions of established design processes and acquisition procedures to counter the Iraqi IED tactics. Over time, the severity of the problem, the relative lack of progress in dealing with it, and the strategic impact it was having were recognized by political leaders. The Secretary of Defense intervened and called for the creation of a formal and structured organization dedicated to defeating IEDs. Congress appropriated large sums of money in supplementals to the defense budget in order to fund the effort. Emergency appropriations were accompanied by increased oversight and political sensitivities.

Most of the early actions of the counter-IED organization concentrated on defeat of the IED at the point of application: up-armoring HMMWVs (High Mobility Multipurpose Wheeled Vehicle), pre-detonation techniques, and jamming radio frequency triggering commands. A cycle of U.S. reaction and enemy counter-action resulted in IEDs getting larger and more sophisticated in both design and employment; armor growing heavier; and jammers chasing the evolving radio frequency, infrared, and visible spectrum for command triggering. As traditional enemy IED effectiveness dropped off, the enemy introduced buried (under vehicle) IEDs and explosively formed projectiles. The Secretary of Defense then forced a shift to a larger, high-ride armored truck, the Mine Resistant Ambush Protected vehicle—an adaptation of a 1980s South African solution to local mine problems.

But it took until 2007–2008 before significant reductions in the IED threat were achieved by a combination of factors, including increased attention to getting to "the left of the boom": the surge (increased presence), turning the local population against insurgents, and surveillance and intelligence operations against bomb makers and insurgent leadership.

Overall Lessons

IEDs should not have been a surprise because they have been used to good effect in previous insurgency wars, including Viet Nam and even as far back as use by the United States against the British in the

American Revolution. Even after recognition of the seriousness of the IED problem and the formation of a Secretary of Defense-backed, heavily funded, high-priority IED defeat organization, the scope of initial response was narrow, concentrating mainly on "point-of-attack" solutions such as up-armoring and command trigger nullification. A much broader approach, including pervasive, persistent surveillance; civilian engagement; and intelligence to neutralize the bomb-makers and insurgency leadership before they have a chance to deploy the devices should have accompanied the rapid response once the seriousness of the IED problem was appreciated.

Case 3. Precision (Global Positioning System) Surprise

Cause

The GPS was originally envisioned for precise targeting for nuclear weapon delivery, with accurate navigation as a side effect. Its development represents the interaction of many streams of research over decades. For instance, physicist and Nobel Laureate I. I. Rabi's invention of molecular beam magnetic resonance in the period between 1938 and 1940 led to the precision atomic clock. In practical terms, the 1965 launch of the U.S. Navy's Transit system navigation satellites (to support the Polaris fleet ballistic missile system) provided experience for the 1973 brainstorming session that produced the GPS concept—a means to support precise nuclear targeting.

In 1978, the first GPS satellite was launched for navigation and precision targeting. During the period between 1978 and 1985, ten prototype GPS satellites were launched. However, before the system became militarily operational, it was adopted in civilian applications. In 1983, after flight KAL 007 strayed into Soviet Russia and was shot down, President Reagan announced that the system would be available internationally for free. By 1984, National Oceanic and Atmospheric Administration included GPS coordinates, spawning the civilian GPS surveying market. In March 1990, selective availability of GPS was activated in order to create a military advantage. However, in August 1990, as the Persian Gulf War started, selective availability was turned off

in order to permit use of commercial GPS units, as military use units could not be produced fast enough. It is estimated that 90 percent of the units used in Desert Storm were civilian models. In 1993, the final GPS satellite was launched, and the U.S. Air Force declared full operational capability in 1995, three years after the Federal Aviation Administration declared GPS sufficient for civilian air travel. Unexpectedly for the military, the GPS had become a civilian-driven capability, causing the military to lose the initial advantage it sought in fostering and using GPS. In time, GPS became a tool that could be used by U.S. adversaries.

Response

The possibility of precise navigation and timing generated many unforeseen applications in both military and civilian domains. Military forces also discovered that GPS aided the execution of military missions unanticipated in the 1973 brainstorming session. GPS received rave reviews from U.S. forces in Iraq during the 1990–1991 Persian Gulf War. Major nation-state militaries around the world have begun to embed precision navigation and timing into their operational concepts, to guide their purchase of weapons and to design their organization for command and control. Non-state actors and terror organizations, *e.g.*, Hezbollah in the 2006 Israel-Hezbollah War, have also found that they can employ GPS to build battle networks that enable precision strikes against their foes. At the same time, the availability of precise navigation and timing has led to the international creation of opportunities for civilian technological innovation, initially aircraft navigation and surveying. Unexpected uses for GPS, such as using the timing precision for coordinating power grids and financial markets, continue to emerge.

Institutional Reaction

The institutional response to GPS has been mixed. In 1980–1982, the program was "zeroed" out due to budget cutbacks and the perception that GPS was not a weapons system. The U.S. political system, in which competing and parallel efforts and programs co-exist, allowed GPS to continue until evidence accumulated to demonstrate its relevance and applicability to developing military missions and tasks. In an effort to preserve the advantage to the military, the civilian signal was dithered starting in March 1990 through selective availability. With

the advent of Desert Storm, the demand for military GPS units exceeded supply—requiring the use of civilian receivers, which were also significantly less expensive, in theater. To facilitate use of the civilian receivers, selective availability was turned off in August 1990. Future GPS constellations will not have selective availability.

Overall Lessons

As could be expected, enemy tactics adapted and exploited GPS. Yet, more important is how quickly GPS moved to an existential technology. Long before the constellation became operational, civilian uses began to influence the technology despite the clear motivation for a specific military use (precision targeting). The current market for GPS technology is about $2 billion. The market size predicted for 2018 is more than $30 billion. While the initial use of GPS was for navigation or localization, newer uses such as coordinating the national power grid and bank transfer depend on timing precision. The interaction of separate technology streams will continue to stimulate novelty and surprise in civilian and military applications. In other words, once a self-reinforcing stream of invention begins, "the tail wags the dog."

Summary Observations: How Well is DOD Prepared for Transition and Fielding Surprise?

The case studies examined suggest that DOD does not respond well to transition and fielding surprise. (See summary of lessons learned, Table 3-2.) The Department neither acts preemptively nor does it plan for resilience in advance of threats—even grave threats—that are not yet obvious or urgent. Further, when the Department does act, responses often take too long. The case of the IED threat is a prominent example. Once the threat became serious, it still took years to field solutions that reduced further casualties. The human and political cost of slow action increased as the situation rose from a tactical matter to one of more strategic importance. In addition, actions taken under the press of urgency may be wrong or incomplete. The case of IEDs again serves as example. Here the Department initially responded with point solutions, such as up-armored HMMWVs, rather than addressing the root cause of the problem by attacking the IED support networks.

Table 3-2. Lessons Learned from Historical Cases of Capability Surprise

Historical Case	Causes	Responses	Institutional Reactions	Overall Lessons	Findings Support
Scud Attacks, 1990–1991 Persian Gulf War	• U.S. did not anticipate Saddam's goals or means • CENTCOM leaders underestimated political and strategic effects	• Senior civilian and military leaders had to focus on strategic and diplomatic issues to exclusion of other tasks • Large military effort devoted to Scud hunt • PAC-2 rushed into production and field	• *Ad hoc* industry and diplomatic response to unanticipated military operation • Modifications required to respond to "urgent need" developed and fielded in weeks rather than years	• Consider enemies geopolitical perspectives stress on own systems prior to conflict	• Rapid reaction capability should be institutionalized • Industry can and will support urgent needs • Experimentation needed to expose vulnerabilities
IED defeat in aftermath of Operation Iraqi Freedom (OIF)	• Saddam's pre-OIF plan for partisan warfare was unanticipated • U.S. didn't recognize use of IEDs in other conflicts • CENTCOM failed to neutralize ammunition dumps	• U.S. used existing tactics, techniques, and procedures; initially regarded IEDs as a nuisance • U.S. *ad hoc* efforts to describe and defeat IEDs solution-based not problem-based • Insurgents watched and rapidly responded to U.S. countermeasures well inside U.S. observe/decide/ respond timeline • U.S. devoted more resources	• Tactical units used informal means to create jury-rigged solutions • U.S. initially used peacetime formal acquisition process to address the IED problem • Secretary of Defense interventions needed to create anti-IED focused response program—initially lacked sufficient clout to cut through bureaucratic roadblocks	• IED use/effectiveness could have been foreseen due to previous use in insurgencies • Secretary intervention required to formalize, accelerate, fund counter-IED rapid-response effort • Even after threat recognition and high-prioritization, the breadth of response was initially narrowly focused to "point of attack" solutions	• Most surprises aren't really new and can be foreseen due to previous experience • Task teams separate from normal acquisition process, with Secretary of Defense backing/priority, are sometimes necessary to focus and accelerate urgent response to surprise threats • *Ad hoc* rapid response organizations sometimes do not visualize/pursue full set of viable response options and focus on narrow, partially adequate solutions
Precision (GPS) Surprise	• 1973: GPS concept for precision nuclear weapon delivery • 1978: first GPS satellite launch • 1985: GPS becomes operational • 1995: U.S. Air Force announced full operational capability	• 1990: GPS enables U.S. battle management system for precision strike in Desert Storm • 1983: Opened for free international civilian use • 2006: Hezbollah used GPS-enabled precision weapon strikes to hold off Israel Defense Forces	• 1980–1982: program zeroed out; budget cuts and perception that GPS is not a weapon system • 1990: Selective availability turned on for military advantage in Desert Storm, then turned off to permit use of civilian receivers	• Enemy tactics adopted and exploited GPS • Civilian uses influenced military development acquisition • New uses continue to proliferate, *e.g.*. power grid, bank transfers depend on *timing* precision	• DOD did not anticipate transition and fielding surprises created by civilian applications

Chapter 3-3. Key Findings Related to Transition and Fielding Surprise

In addition to careful examination of the three case studies in the prior chapter, the panel was further informed of DOD's ability to address transition and fielding surprise through interviews conducted with representatives of industry, government, and the intelligence community, as well as by review of relevant documents and previous studies. All of these sources and accompanying analyses formed the basis for the findings discussed in this chapter.

As a result of this investigation, the panel's principle finding is that:

> ***DOD has long recognized the inadequacies of its mainstream acquisition system in dealing with quick reaction needs. However, DOD's internal decision-making processes and ensuing action chain for identifying and rapidly dealing with high priority surprise are inadequate and can be substantially improved.***

This finding is elaborated with more specific findings and discussion below.

Finding 1. Lack of Integrated Processes and/or Organization

DOD lacks integrated processes or an organization with a mission to anticipate, collect, and address transition and fielding surprises.

There are several core challenges that make the current DOD structure and business processes unable to adequately address the kinds of threats posed by transition and fielding surprise:

- **There is no recognized, focused responsibility or process to anticipate and prioritize transition and fielding surprise as an ongoing mission.** This kind of

process would identify and address military or other U.S. government transition and fielding needs that will arise with little or no warning, or require action based on anticipated threats, likely without full or clear justification in the traditional needs process.

- **As a corollary, there is no process to assess and assign action priorities and funds to address extraordinary surprise of any kind**, especially in addressing threats that are novel, cross-Service, extraordinarily urgent, or potentially grave but not yet proven. Today these kinds of surprises are lumped with other types of urgent needs and prioritized by operational or acquisition offices that may not have a wider view of the context and potentialities of the surprise threat. Even urgent requirements processes are often saddled with bureaucratic approval criteria, processes, and chains. Further, these processes become loaded with needs that range from minor to major, and the priorities for addressing urgent surprise needs can be unclear. The result is that surprises can be misunderstood and poorly prioritized for action, until a surprise escalates to increasing urgency or danger.
- **There is also no focused interface with the intelligence community.** As a result, DOD reacts in a way that is fragmented and cumbersome, and is at risk of being unable to effectively deal with impending threats. This position is unacceptable for DOD in the context of today's "persistent conflict," very high probability of surprise, and ease of adversary transition and fielding development.

As a result, the Department is often caught flat-footed and/or slow to recover. Characteristics of initial response include the following:

- Lacking an integrated process for anticipating transition and fielding surprise, DOD often does not take strong preemptive steps or plan well in advance for transition and fielding resilience. Instead, the Department tends to wait until the threat signals grow more urgent before responding.
- Urgent transition and fielding surprise responses often stumble at the interfaces for decision-making, either between the user and acquisition communities or within the DOD acquisition and

contractor community itself. As a result, DOD operational commanders becoming reactive, approaching the acquisition system for rapid point solutions.

- Decision-makers establish priorities for action based on information they have at hand about the surprise, but this often is not the full context in which the surprise threat is occurring. In addition, due to the urgency of the situation, it may not include a full context for solutions. The result is that an action response may take longer than needed or be incomplete in addressing the full threat.

Finding 2. Inadequacies of mainstream acquisition for rapid response

The mainstream DOD acquisition system and business processes are not well equipped either to anticipate or respond to urgent needs—they are inadequate to meet challenges in a world that moves more quickly than a 10-year development cycle.

DOD's formal system acquisition process is not designed to anticipate and/or rapidly respond to adversary surprise. DOD's business processes—including its budgeting, requirements, and contracting processes—are risk-averse and intended to support large, high-cost, high-complexity systems development and production programs over extended periods of time. DOD's acquisition system was established and modified over decades to produce very sophisticated capabilities within a disciplined and controlled set of processes. The system is also designed to provide extensive transparency in the expenditure of public funds to ensure legal and policy controls are met.

With these legal and fiscal demands comes a significant amount of oversight and administrative burden. The DOD acquisition system brings with it extensive scrutiny of program and contract actions, and creates an approach to problems and programs that is risk-averse both inside the Department and in its primary supporting industry. The issues associated with programs managed within the DOD 5000 acquisition system have been well documented in numerous prior

studies, including many by the Defense Science Board. These issues and findings will not be repeated or addressed here, nor is there any attempt to redress the deficiencies outlined in these many previous studies. Nevertheless, DOD must improve the responsiveness of the existing acquisition system. In the three case studies the panel examined (discussed in the previous chapter), DOD relied on exceptional responses involving senior Department leadership who recognized the need and were willing to by-pass mainstream processes in order to deal with exceptional transition and fielding capability surprises.

The central point is that this acquisition system was not designed to, nor does it adequately address, the kind of "on the edge" threats that transition and fielding, or indeed some of the other kinds of surprise, represent. To respond appropriately, the acquisition approach to address critical surprises must be extraordinarily agile, adaptive, able to field new or adjusted capabilities with great speed, and able to reform its shape and resources dynamically. It often cannot wait until threats are fully apparent and vetted through long requirements chains. It also often cannot wait until solutions are defined, perfected, and proven to meet the rigors of DOD standards, processes, and specifications. It must act in context of the full surprise situation and quickly deploy a solution that best meets or mitigates the threat at hand. It is this critical balance between speed of response, extent of oversight, and "good enough" performance that is missing in today's system.

Finding 3. Limitations of Existing Rapid Fielding Organizations

The DOD acquisition and user community's many rapid reaction and fielding programs and organizations are *ad hoc* and fragmented, and do not have the mission or scope to address the larger, ongoing transition and fielding surprise threats facing DOD today and into the foreseeable future.

The DOD acquisition and user communities have created many rapid reaction and fielding programs and organizations over time to allow faster responses to urgent needs. Each Service and many operational organizations have been forced to stand up *ad hoc* solutions

to respond to urgent needs, given the lack of institutional capability to address surprise. But because of their *ad hoc* nature, these organizations are not consistently providing an integrated decision and response chain with robust follow-through. Furthermore, there are no "sunset clauses," so that the organizations tend to persist even after the original needs are addressed.

With an anticipatory capability, surprise can be preempted or rapidly mitigated by forward-looking responses before the situation becomes urgent. The current DOD "rapid reaction" programs do not address the need for ongoing acquisition processes or a core group assigned with an ongoing mission for extraordinary surprise anticipation and response.

While the DOD acquisition system is generally characterized by independent assessments and process participants alike as slow and ponderous, it has, in fact, been made to perform many times to provide rapid solutions when the urgent priority or emergency nature of the problem warranted. When urgent needs demand, DOD operational and acquisition managers have used every means available to overcome or work around bureaucratic barriers and solve the problem. This can be understood by those familiar with many successful "black" programs. **In cases where extraordinary measures were demanded, DOD has put focused leadership, funds, the right culture, and the right skilled people on the mission and made it happen.** However, these are not cases where the "normal system" was allowed to do its thing, but where leadership intervened to enable the right kind of managers to act and absolutely demand fast performance by working beyond the normal system in all ways possible within the law.

In fact, today DOD has established dozens—some estimates say 20 or more—rapid reaction, rapid fielding, and rapid technology insertion/transition programs (see Table 3-3 for examples of such programs). All of these programs are attempts to "side step" the normal DOD acquisition system in order to meet threats and field needed capabilities more quickly. The fact that the Services and combatant commands need such programs strongly underscores the unaddressed system-wide need for a better process to solve urgent requirements.

Table 3-3. Examples of DOD Rapid Fielding and Response Programs

Example Programs (not all)	Organizations	Cons	Other Recent DOD Analyses of Rapid Programs
Rapid Response to Warfighter • Joint Capability Technology Demonstrations • Joint Rapid Acquisition Cell • Rapid Reaction/ New Start • Rapid Equipping Force • Warfighter Rapid Acquisition Program • Rapid Technology Transition • U.S. Marine Corps advanced technical demonstrations • Joint Improvised Explosive Device Defeat Organization	• Director, Defense Research and Engineering/Office of Advanced Systems and Concepts • Director, Defense Research and Engineering/Rapid Reaction Technology Office • U.S. Army • U.S. Air Force • U.S. Navy • U.S. Marine Corps	• Many small programs requiring hand management by senior leaders all over DOD • Painful learning about speed repeated for each program (contracting, legal); processes reinvented • Funds often "found" fallouts from normal budgets; often resort to seeking earmarks • No DOD process for periodic assessment to determine need to continue or drop program • Rapid programs often treated as "one-off/low priorities" by programs of record • Diffused efforts, most without scale to leverage	• Rapid Acquisition Process Analysis (Deputy Secretary of Defense initiative; FY09 National Defense Authorization Act, House Armed Services Committee request) • Assistant Deputy Under Secretary of Defense for Innovation and Technology Transition (ADUSD (I&TT)) Strategic Initiative on Innovation and Technology Transition [Under Secretary of Defense for Acquisition, Technology, and Logistics initiative] • Army Science Board 2008 • Government Accountability Office audit of DOD ability to meet war fighter urgent needs • Defense Science Board Task Force on Fulfillment of Urgent Operational Needs, 2009
Technology Transition and Fielding • Technology Transition Initiative • Defense Acquisition Challenge • Foreign Comparative Testing • Defense Production Act Title III • Defense Venture Catalyst Initiative (DaVenCi)	Director, Defense Research and Engineering (various organizations)		
Technology Transition Programs/Lead Offices	U.S. Navy, U.S. Air Force, U.S. Army		

DOD managers are struggling to find any means possible to work around the highly disciplined but ponderously slow system to create responses more quickly, while U.S. adversaries are able to deploy every means possible with little process or discipline—possibly sloppily, but to adequate effect—to adapt or adopt technologies to target U.S. vulnerabilities. Even adversaries with bureaucratic acquisition systems of their own can now more quickly adopt and field an asymmetric capability to target U.S. weapon systems moving through their ponderous acquisition cycles.

High priority capability surprises, when there is no organization clearly responsible to address them, are dealt with through *ad hoc* organizations set up by the Services and agencies, by the Joint Staff, or by direct order of senior Department officials. When such rapid response "bypasses" to the normally cumbersome budgeting, requirements, and acquisition processes are established, other operational needs, often not directly related to the original mission of the organization, become candidates for "special" treatment, blurring the original rapid response mission and resulting in rapid expansion of the organization. This ultimately defeats the original intent, as too many needs become priority needs.

As an example, the years of operations in Iraq and Afghanistan have resulted in the creation of many rapid response programs, as the operational commands and Services have struggled to meet needs arising urgently and unexpectedly. One such program is the Army Rapid Equipping Force (REF), a service-level program established by the Army to meet Army-specific needs. The REF evolved from a mechanism to deploy Packbots (in 2002) into an operating arm of the Army user community to address urgent needs arising, most notably from operations in Iraq and Afghanistan. Today they cite their scope as "anywhere [Army] soldiers are engaged," and are now addressing other urgent needs wherever the Army is operating.

The REF has cleared many "normal" system roadblocks and has a number of attractive features:

- It can accept requirements submitted informally (using a "10 liner" requirement statement when needed) and verify back to the requester quickly—within days if need be—so the operational submitter knows his/her request is getting attention. The REF begins to quickly assess the need, and in parallel seeks appropriate Army review and approval for a project via the Army's established process for urgent needs. But the REF goal is to keep approval and solutions moving to address truly urgent needs.
- It is led by an operational 06-level officer (colonel) with a strong passion to respond to the Army operator needs. It also has field operational support teams to interact on the spot with the field needs.
- It has some decentralized spending authorities for amounts below $3 million and can fund from many types of accounts, including research, development, test and evaluation; procurement; and operations and maintenance. For higher cost solutions, a more formalized Army review and approval is needed.
- Before creating a new response, it consults with other Army organizations to determine if someone else is addressing the need already, and will meet user needs rapidly enough.

But the REF is limited by factors that plague many similar programs and organizations inside DOD:

- Its funding base is set by what can be assigned versus what is needed. The difference has been made up by relying on supplemental funding now—it recognizes that source could go away.
- It resides in the user community staff, outside the acquisition community (which has pros and cons) and has few acquisition-skilled people assigned. It has had three different procurement support organizations in its short lifetime. Its contracting support organization does not necessarily specialize in speed and non-traditional contracting, and does not typically know or deploy tools such as Section 845 "other transaction authority." The REF continues to struggle with the procurement community to keep its speed up and not be burdened by "normal" DOD contracting approaches with their risk-averse

bias. As the REF continues to grow, it is likely to become subject to many of the procedural and bureaucratic controls that it was originally established to avoid.

- It had to scramble for staff when established and ramped up, which means it leans heavily on contractor support (as does JIEDDO and other such recently established organizations).
- Its mission and current budget (even that outside the supplemental) may or may not continue as the conflict in Iraq grows less intense; it will try to survive but its future is unclear.

The needs from the responses to the Iraqi and Afghanistan conflicts may diminish, and the Army's need for the REF along with them. But each time programs such as the REF are set up and stood down, DOD introduces the risks of leaving ongoing urgent needs unaddressed and lessons learned lost. Further the REF is only one of nine such programs identified by the Army and of many more that have been operating DOD-wide. Each point solution program may serve a good purpose, but many have been created in isolation and in a reactionary mode. They are not motivated to learn best practices from each other. None is focused today in service of the larger mission of dealing with surprise—transition and fielding surprise or any of the other types that this study examined. Of particular interest is that none of these 20 or so programs has the anticipation, prevention, and/or mitigation of surprise as its charter, nor do they have the field of view or DOD-wide authorities for such a mission.

Recognizing that the increasing incidence of rapid reaction programs being established in the Office of the Secretary of Defense (OSD) and the military services points to an enduring, and likely increasing, demand for more speed in response to urgent needs, several leaders in DOD have undertaken a review and assessment of these types of programs and organizations. For example, under the auspices of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)), OSD is leading a "Lean Six Sigma Analysis" with all Service and OSD rapid response and technology transition programs. The Army Science Board (ASB) 2008 Summer Study assessed the nine Army rapid response capability programs. The ASB is assessing how to create an Army Rapid Response Capability in response to a sustained requirement. They are

recognizing that the nature of the threat today is different and that "in an era of persistent conflict, the Army may need to institutionalize a rapid adaptive organization, rather than reinvent ad-hoc approaches for each new period of high intensity demand Army." Both the OSD and ASB reviews are assessing whether some number of existing rapid response and technology transition programs need to end and others sustained and leveraged into an ongoing institutional response capability, with ongoing mission, staffing, and budget authorities.[35]

But even before these recent studies were initiated, the Defense Science Board, in its 2006 summer study on 21st Century Strategic Technology Vectors, recognized the enduring need for a rapid response capability, writing that the Department should " … create a single new entity, the Rapid Fielding Organization … to provide funding for rapid fielding, sustainment, and transition [of new capabilities] to the military … ."[36]

The barrier in DOD to effectively addressing surprise is not that U.S. laws and DOD acquisition organization or processes can never work with speed and agility. The barrier is that DOD has not created or organized a process and rapid response capability that has a continuing mission focused on the threat of capability surprise, where exceptional, novel, and unusual solutions or extraordinary responsiveness are demanded and where routine rapid acquisition and fielding needs are handled satisfactorily with existing mainstream organizations.

---

35. OSD's Lean Six Sigma Analysis recognized that small, focused organizations have successfully addressed immediate warfighter needs, but recommended institutionalizing the process for how such organizations should operate. Detailed recommendations focused on prioritizing urgent needs, timely decision-making, funding, training, and accountability through common metrics and data availability. The Army Science Board study concluded that innovation needs to be a separate function in the Army and recommended establishing a Deputy Chief of Staff for Innovation (G-9), who would be responsible for sustainment and transition of rapid innovation to support operational needs.

36. *Defense Science Board 2006 Summer Study on 21st Century Strategic Technology Vectors, Volume IV. Accelerating the Transition of Technologies into U.S. Capabilities*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, April 2007, p. v.

Chapter 3-4. Actions Needed to Redress Transition and Fielding Shortfalls

Managing surprise can be viewed as an exercise in risk management. DOD must deal with a wide variety of known and potential risks, some of which mature into anticipated threats, some of which never mature, and some of which arrive as surprises, either as peacetime threats or during war. But while some risks are adequately provided for by current processes within DOD, there is no overarching, ongoing process for anticipating or addressing those that arise quickly as a result of capability surprise. There is also no senior level organization that specifically assesses DOD-wide risk vulnerability, and no central organization designed to provide rapid reaction to the highest level of surprises that must be dealt with expeditiously.

To fill this deficiency, the panel believes that DOD should establish new processes for anticipating, collecting, and responding to high-priority surprises, including surprises that arise from transition and fielding as well as others. Existing DOD organizations, including mainstream Services or agencies, should be held responsible for countering these surprises where possible. They must determine how they can better handle surprises through the normal course of affairs. However, extraordinary challenges will require action by exceptional teams with direct involvement of the Secretary of Defense. Figure 3-1 outlines the process envisioned by the panel at a top level. DOD needs to organize to reduce the risk of capability surprise and to provide a mechanism for extraordinary rapid reaction more quickly than normal budgeting and requirements processes permit.

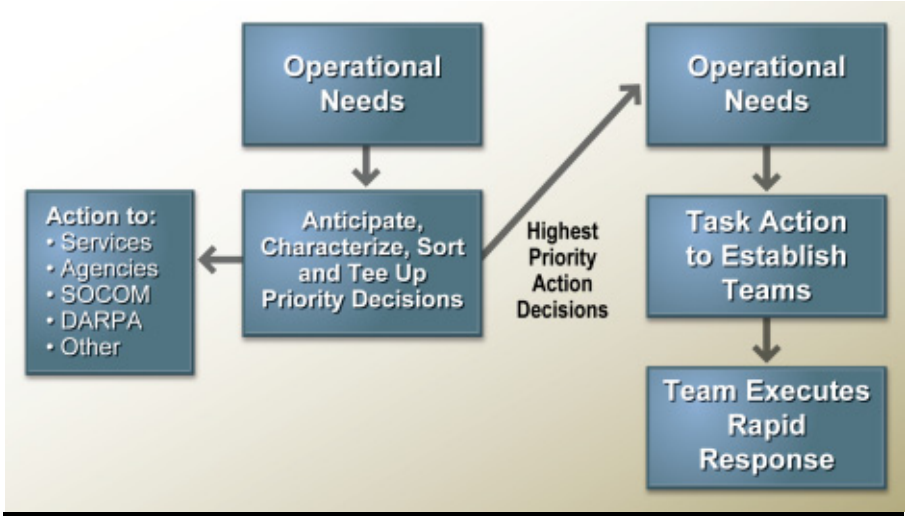


Figure 3-1. Process for Responding to High-Priority Surprises

In forming its recommendations, the panel sought to address the capability surprise challenge keeping several precepts in mind:

- Establish an overall process for quickly identifying and responding to capability surprises with the ability to react extraordinarily fast in a few, high-priority instances.
- Establish a single analyzing, sorting, and decision process for capability surprises, anticipated or realized in the field.
- Assign responsibility, as appropriate, to existing organizations within DOD.
- Identify those truly exceptional surprise challenges deserving of extraordinary response.
- Create a minimum of new standing organizations and rely on small, temporary, very focused teams to solve extraordinary problems.
- "Clear the decks" of routine procedural friction and make best use of means for expediting projects.
- Hand over results at project completion or at pre-determined milestone achievement to appropriate Services and agencies to sustain and support.

The recommendations presented in this chapter aim to give a "jet-assisted takeoff" to extraordinary rapid response needs and to make best use of existing DOD capabilities in handling responses they can address, as exceptional capabilities already exist in the Department and its contractor base. The panel recognized that there are many ways to organize and manage the needed processes, and offers its own proposed approach.[37]

RECOMMENDATION 1. CREATE A UNIFIED PROCESS AND ORGANIZATION TO DEAL WITH HIGH-PRIORITY SURPRISE.

The Secretary of Defense should create a Capability Assessment, Warning, and Response Office (CAWRO) charged to establish and carry out a unified process for anticipating, collecting, analyzing, and managing urgent, militarily significant capability surprises.

DOD has no established or integrated process for dealing with truly high-priority surprises in a rapid manner. The intent of this recommendation is to instantiate a flexible analysis, prioritization, decision, and rapid response process that can address the most urgent, militarily significant needs. The CAWRO should report directly to the Secretary of Defense. This office would have the role of assessing the adequacy of DOD's risk mitigation activities and of identifying risks that may not have been adequately addressed. It would make recommendations to the Secretary of Defense about specific courses of action that should be taken in response to these risks and in response to capability surprises that manifest themselves. The CAWRO should not be constrained from considering or acting on any anticipated or realized capability surprises. However, it should not be regarded as the sole surprise management organization. Services and agencies, as appropriate, may often be the most appropriate response organizations.

The CAWRO's process should address and prioritize all surprises not handled in the normal course of operations by operational forces or their supporting Services. In analyzing and managing surprises that

37. Note from the study chairs: The Transition and Fielding Panel's recommendations are consistent at the top level with what the overall study recommends in the main report (Volume I), but as with the other two panels, some of the details differ.

come to its attention, both anticipated and encountered in operations, the process should assign responsibility for responding to standing DOD organizations best able to address each surprise. The few surprises that standing DOD organizations cannot adequately address (*e.g.*, because of urgency, scope, or nature) should be brought before the Secretary of Defense for special consideration as an extraordinary rapid response effort.

The prioritization process should review all available solutions to a capability surprise, both defensive and offensive. Via a prioritized assessment process, determination should be made as to which options, if any, might meet the surprise challenge and its projected second and third order effects. A recommendation should be brought forward as to which one is "best," what best means in this context, why it is best, and how the other options rank in relation to it.

The range of available management options includes:

- Decision made by on-the-scene commander—ignore nuisance "surprises."
- Innovative uses of resources already available to the combatant force—solve/counter surprises in-theater.
- Program office/acquisition system makes near-term improvements—straight-forward up-grades or modifications of existing production systems/practices that can be made through an existing program office or Service acquisition system. Services develop training and operational adaptations.
- Create or develop new variations by Service acquisition organizations/AT&L—new enhancements or revisions to existing products or technology, such as adaptation of an existing system (*e.g.*, Patriot) to address new threats (*e.g.*, Scuds). Such changes require new confirmation, training, fielding, and support.
- Develop Special Operations Command (SOCOM)-type specific response—operational or acquisition counters to surprises that are bounded or single event requiring quick response.
- Develop new technology from the Defense Advanced Research Projects Agency (DARPA)/larger research community/

industry—technology surprise efforts that require significant analysis and research and development (R&D) efforts. CAWRO might delegate response to DARPA, federally funded research and development centers, or other elements of the R&D community.

- Establish rapid response team for new project effort—CAWRO and the Secretary of Defense conclude that no existing DOD organization or capability at hand is able to provide timely fielded counters to current or projected urgent, high-priority surprises.

Figure 3-2 depicts CAWRO's sorting process for capability surprises—a "triage protocol" for responding to surprise. Any surprise above a nuisance is filtered into solutions (arrows reflect how the solution approach will be executed by the corresponding entity). Not all surprises will require a formal response, but significant surprises will certainly require CAWRO to engage existing agencies or communities and the rapid response group. Extraordinary surprise may elevate the response decision to the Secretary of Defense level.

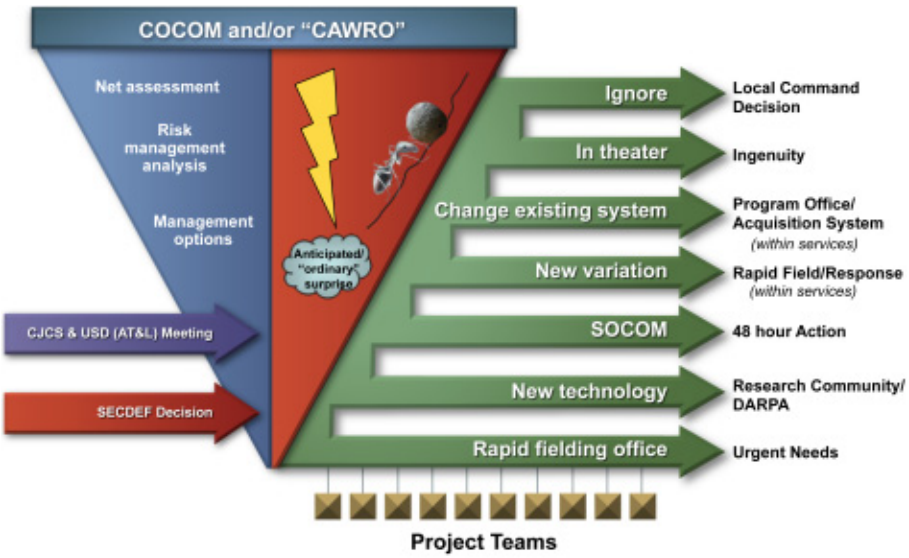


Figure 3-2. "Surprise" Triage Process

When CAWRO encounters capability surprises that do not fit existing DOD competences, it enters into a process leading to a decision by the Secretary identifying the threat as a priority issue and authorizing extraordinary efforts to address it.[38]

RECOMMENDATION 2. ASSESS SERVICE AND AGENCY RAPID REACTION NEEDS

DOD should determine the rapid reaction needs of the Services and agencies and establish the organization required to meet them.

Regardless of any action taken or not taken on the CAWRO (Recommendation 1) or on establishing a new rapid response capability, the Department needs to complete a review of existing rapid response organizations and programs within OSD and the Services, and consolidate or eliminate where appropriate. The USD (AT&L) and the Services are encouraged to continue their current, ongoing reviews of DOD rapid reaction and technology programs and organizations. The reviews should determine which rapid response and technology transition will continue, which should be combined, and which should be eliminated. This panel recommends that, once this DOD review of current organizations and programs is complete, the Department should move to create a formal Rapid Response Group reporting to the Secretary of Defense (Recommendation 3). However, there will still be a need for standing rapid reaction capabilities to handle routine needs of the Services and agencies.

38. Appendix 3-A describes the function and decision-making process of the CAWRO in further detail. In addition, part of the CAWRO's success will depend on a strong partnership with the intelligence community. Appendix 3-B elaborates on this point.

RECOMMENDATION 3. CREATE A RAPID FIELDING CAPABILITY

The Secretary of Defense should create a Rapid Response Group within the CAWRO with skills in quickly forming, managing, and supporting rapid response teams.[39]

This third major panel recommendation creates the process for translating the Secretary's decisions into fielded solutions to counter capability surprises. When a surprise has been elevated to the Secretary of Defense and an extraordinary rapid response effort designated, that effort has the Secretary's support for expedited funding, staffing, resources, and acquisition. The Secretary of Defense decides that a rapid reaction team approach is called for, and the Secretary, with CAWRO support, provides guidance to the Rapid Response Group to commence with formation of teams.

Based on its experience, and the realities of large organizational behavior, the panel concluded that truly exceptional challenges (those selected by the Secretary of Defense) demand exceptional teams and capabilities to expedite response. The core function of the Rapid Response Group provides the expertise in establishing, supporting, and managing focused rapid-response teams quickly and effectively to address objectives set forth in the Secretary's decision. It must have unique budgetary, acquisition, legal, and support capabilities to enable the rapid response teams to mobilize resources needed to develop, produce, and field urgently needed counters to surprises.

The rapid response teams should be focused on response objectives, be small, agile, and operate in a "Skunkworks" management style, using expedited funding, requirements, and acquisition means, supported by the Rapid Response Group. The teams should have a defined lifetime. At the conclusion of their work, the rapid response teams transfer the

39. The main study considered this option along with others. Although the Rapid Acquisition and Fielding Organization (RAFO) (the name ultimately decided upon by the full study) bore many of the characteristics described here for the Rapid Response Group, for the reasons cited in Volume 1, it was recommended that the RAFO should be a separate organization from the CAWRO reporting to the USD (AT&L).

results of their efforts to appropriate Services and agencies for continuing development, sustainment, and support.

The rapid response teams plan, develop, produce, and field counter-measures to the capability surprise as fast as possible, unhampered by procedural friction. Each team must identify and work with one or more Service or agency clients from the onset of each case for action. At the conclusion of the rapid response team's mission, its work and the responsibility for training, support, and further development is transferred to the appropriate client Service or agency to continue to maintain the newly developed counter-surprise capabilities. After successful transition, the team will disband. Each extraordinary rapid response team should be unique to its challenge and should be temporary in duration.

The panel evaluated several organizational structure and placement options for material solution execution teams (see "Framework" section following the recommendations). However, as important as placement and organizational structure are, they are secondary to the ground rules, charter, and support structure that govern an execution team's work. Those ground rules must facilitate and enable execution consistent with the urgency and objectives required, and be tailored to the specific problem and approach adopted.

Teams or organizations charged with the execution of high-priority urgent surprise response projects should not be constrained by rigid institutional roles, responsibility, and authority concepts. In large part, ongoing established DOD organizational structures are designed to ensure normal operations are executed within sets of ground rules designed to minimize variability and execution risk—if you will, to support the equivalent of "batch" processing. The effect is reduced tolerance for risk in favor of generally accepted procedures; distributed responsibility; numerous levels of review and long approval, planning, and funding timelines.

The impact of this natural institutional bias is that decisions, tools, and timelines are "optimized" at the aggregate level for non-urgent tasks, and not at the specific program or project level. The dominant culture is to push to a one-size-fits-all approach, despite the existence of tools designed to allow expedited execution. In urgent situations, DOD

managers seek to find and implement rapid response efforts within existing means, but such efforts tend to be an uphill struggle against the "normal" mode of business. Over time, unable to provide low latency between needs, actions, and results, such efforts are sapped of their effectiveness.

Truly exceptional rapid response success requires that strong, clear ground rules be in place and consistently supported. The first, most critical ground rule is that the charter, tasking, and urgency must come from, and be vigorously supported and reinforced at, the Secretary of Defense level. Without such top-level, exceptional support, the tendency of any established organization will be to "normalize" the execution process, ultimately destroying its ability to perform its mission. We strongly urge that rapid response team charters and support be tailored to their tasks and sponsored at the most senior level to assure focused, rapid, and tailored execution.

The rapid response teams will face new challenges in working with the private sector to field the best possible solutions in the least possible time. Large, traditional defense firms have scale and are savvy in DOD contracting and management demands. Certainly, established defense suppliers have background experience and scale to support rapid response needs, but they may not have novel or unusual solutions that best address unique or "on the edge" surprise threats.

Solutions to unusual challenges may often reside in small firms, independent laboratories, and other non-traditional defense providers. But smaller companies and other non-traditional suppliers generally lack scale or ability to form traditional DOD relationships. Rapid response teams must be skilled in finding and dealing with unconventional providers or "marrying" them to large-scale, more traditional defense suppliers if the scale of response or other special circumstance so warrant.

Framework for Handling Surprise and Extraordinary Risk

Table 3-4 summarizes the overarching framework for recommendations 1 and 3:

- The CAWRO is charged with anticipating and collecting surprise data, developing courses of action to respond to surprises, and bringing to the Secretary of Defense options to deal with exceptional risks or surprises.
- A Rapid Response Group is the core mechanism to implement decisions made by the Secretary of Defense in which rapid fielding of a new or modified capability is called for. The Rapid Response Group establishes rapid response teams to develop, produce, and field counters to surprise.

The unique expertise in the rapid response organization will be the ability to do things fast, outside normal funding, requirements, and contracting constraints. "Ready reserve" domain specific expertise will be drawn from established DOD and contractor organizations and from the outset, the team will plan for transition to existing organizations for sustained life cycle support.

The Rapid Response Group and rapid response teams must work in an environment that encourages free-thinking, imagination, and a willingness to take intelligent risks by pushing the envelopes of thought and concepts—a venue where failures of intelligent risks are not penalized. The group and each team keep the system informed proactively but use ground rules to limit distractions or diversions. The teams have the charter to call on support from other parts of DOD as needed. (Further detail on the rapid response operating concept is in Appendix 3-C.)

Table 3-4. Framework for Handling Surprise and Extraordinary Risk

Anticipate and Synthesize Surprises: CAWRO	Deal with Surprises: Rapid Response Group
Institutionalized Vision • Understanding cultures and intent • Self-vulnerability assessment • Broadly focused indications and warning • Selectively focused intelligence • Global think tank and doctrinal input **Defensive Competitive Strategies Evaluation** • General threat definition • Pre-emptive red-teaming, experimentation, and operational gaming • Potential damage assessments • Potential system/operational response assessment **Offensive Competitive Strategies Evaluation** • General opportunity postulation • Red teaming, experimentation and operational gaming • Potential payoff assessment • Potential offensive system/operational assessment **Decision Support** • Risk assessment, prioritization • Options generation and budget estimates • Decision memorandum to Secretary of Defense	**Rapid Response Incubator** • Rapid response team formation and support – core hotel functions – tech manager “rolodex” and directory – colorless money – urgency culture and rules – non-traditional sourcing and outreach **Response Task Management** • Tactics, techniques, procedures formulation • Resilience/robustness installation • Operational system adaptation • Rapid countermeasure development and fielding **Field Testing and Operational Feedback**

The desired features of the rapid response teams are as follows:

- **Management approach.** Teams are delegated both authority and accountability with clear goals and objectives stated. The emphasis is on speed over other factors, with emphasis on short lines of decision-making. The teams have high priority for resources of all types—laboratories, ranges, people, and equipment—both internally or by reaching out to other communities. Performance incentives will apply to both internal staff and for contractors. The teams will have limited oversight.
- **Leadership.** A leadership cadre is competitively pre-selected. They are assigned by senior leadership based on specific risk expertise and availability.
- **Quality technical and management staffing.** The small, agile teams are put in place rapidly with hand-picked staffs drawn from a career enhancing, competitively selected staffing pool.
- **In-place "housekeeping" structure.** The teams are supported by streamlined contracting, flexible funding (including colorless, multi-year dollars), and a database on national expertise.
- **Termination.** Teams are established with a sunset clause to end or transition activities to "normal" processes and organizations.

The panel debated several options before recommending the approach described. Options include incorporating the rapid response capability in an established organization such as DARPA or other Service materiel commands and laboratories, or establishing a new dedicated R&D agency. Both these standing organization options have serious drawbacks. The demand for urgent responses to high-priority surprises or vulnerabilities is neither predictable nor steady and would not be a frequent occurrence; most risks and many surprises are adequately managed by existing offices or field organizations. For those exceptional risks demanding a highly responsive approach, merely allocating responsibility to an existing organization is not adequate—the routine business and management culture will stymie unconventional approaches needed in exceptional circumstances. On the other hand, a new centralized agency could never be expected to have all expertise needed to

address problems that might arise. The panel rejected both of these options in favor of a more streamlined and flexible approach.

Rapid response approach options can be likened to an active duty force consisting of a standing, full-time professional fire department versus an incident response force—a fire department with a small core cadre of full-time employees for maintenance and a diverse pool of available response resources on call. The professional department covers the bulk of routine incidents; the incident response force takes on those events requiring special skills or methods. Given the diverse nature of anticipated demand and the spectrum of resources that could be brought to bear on any given problem available throughout DOD, but located in no single organization, the panel concludes that the incident response force concept with a small core cadre is the preferable approach. This organizational design allows the Department to capitalize on the wide spectrum of existing resources as needed. The panel did not support a standing agency that would duplicate existing DOD technical and management capabilities.

The recommendations above reflect an organizational design consisting of a small core cadre Rapid Response Group, composed of housekeeping functions (contracting, personnel, and financial management) and administered by the CAWRO that would enable rapid formation of appropriately tailored task forces, or rapid response teams, designed to address specific problems. The teams would have immediate access to needed capabilities within DOD, with a streamlined execution capability. This approach best institutionalizes a rapid reaction capability for very high-priority surprises or risk mitigation.

Chapter 3-5. Challenges in Creating an Effective Rapid Response Program

A number of challenges will present hurdles in terms of establishing and executing an effective rapid response program. If the program is to succeed, these challenges, both internal and external, must be met and overcome. An overarching consideration that has to be injected into the system is the ability to balance the risk associated with delays in providing a needed operational capability with the risk of providing that capability in a less-than-standard manner that does not provide all of the conventional "bells and whistles."

Internal DOD Challenges

The panel considered challenges to effective rapid response programs and addressed how they can best be managed, the results of which are listed in Table 3-5. Many of these challenges are related to the acceptance of "jump start" rapid response teams by existing DOD stakeholders and the mechanics of implementation, funding, and sustaining support for the approach. In general, the panel tried to define the Rapid Response Group as an enabler of rapid response outside the normal requirements and budgeting process, but not as an organization that could be regarded as a competitor to that process. The bulk of development, transition, and fielding programs would still be met by the standard process. Rapid response teams would be established only when a surprise could not be adequately countered by existing DOD resources (either in capability or in expediency).

In addressing an on-going mission to provide new or modified operational capabilities to the field very rapidly, DOD must gather lessons learned from past rapid response efforts and assess the strengths of its organizational capabilities to be creative and circumvent "status quo" thinking and processes. Gathering and understanding lessons and organizational capabilities should be an on-going role for the Rapid

Response Group to assist in its role of establishing and supporting rapid response teams.[40]

Table 3-5. Implementation Challenges

Sustaining the desired environment in the face of bureaucratic pressures	• Requires senior leadership commitment and perception of value added
Avoiding a full core that would be idle much of the time	• Surprises are intermittent and not predictable • Most risks are being addressed in the "normal" system • Only a small core team is needed
Preserving the small core that is required	• Can provide housekeeping services on demand • Knows how to conduct streamlined contracting • Manages the human resources system—maintained leadership and key technical resources pool • Place the core team within OSD in an existing shop—a USD (AT&L) organization
Avoiding internal and external "natural enemies/competitors"	• Utilize service-led task force organizations as appropriate based on domain expertise, funded from OSD • Only use OSD-based task force if problem solution approach is truly novel • Establish cooperative relationships with Joint Staff, OSD offices, intelligence community, and Services
Provide for transition into "normal" production, training, logistics support	• Must be part of project planning and must have support of receiving organization
Operational community support/acceptance of "solutions"	• Must integrate relevant operators into the task force • Solutions have to work in the field

40. One challenge—dealing with software surprise—was outside the range of issues DOD normally deals with in the political, management, and bureaucratic environment and, in our view, was deserving of much more detailed discussion than the panel was able to provide during the course of the study. The unique nature and challenges of dealing with surprises where software is a major consideration are discussed briefly in Appendix 3-D, but deserve much more attention.

External Challenges

DOD will need to address the unique risks to industry and other solutions providers for very rapid response to surprise. Finding and fielding rapid solutions to urgent DOD requirements is not a novel problem. The Department often taps firms or laboratories to address its rapid needs. The Department and its rapid response teams must develop efficient practices and policies to use industry and independent laboratory partners. DOD can be poorly attuned to smaller company business needs in establishing their contracting and risk management and payment policies, and tends to treat large and small firms alike regardless of their size or nature. Of particular concern is the impact of payment policies on the financing and cash flow of small firms. Well-intentioned actions by program managers or contracting officials can inadvertently damage otherwise successful smaller firms.

Larger, more traditional defense firms may pose different rapid response challenges. They may choose not to participate in projects they consider too niche or "one off," or be unwilling to put up capital (even if they have scale) for a production they see as having no long-term future market or pay-off. Major contractors also have larger organizational issues to deal with and possibly conflicting priorities and interests. Would a firm take on a small, novel program that might end up serving as a rival to its larger program of record? What incentives might circumvent this problem?

Regardless of the size or nature of a firm or source supplying rapid solutions, rapid response teams will face challenges that require them to step outside normal contracting, funding, and management models. As new teams are set up, they will need to carefully judge and assign risk, considering the size and nature of the supplier and the urgent demands the Department is placing on it. DOD may need to facilitate teaming to achieve its goals of innovation and timely transition of a solution to the field. In developing contracting and funding strategies, rapid response teams should employ some of these tools:

- When there is time to solicit a request for information or other initial screening for concepts, options, or solution approaches, DOD should fund the request for proposal work after the initial screening so that the supplier does not bear the up-front

funding burden immediately. If not, the Department may lose out on some sources that will not or cannot afford to bid.

- Canvas very broadly to seek potential solutions. Include foreign firms and laboratory solutions. DOD can perform classified missions with commercial and sometimes even foreign firms if managed properly.
- Make funding and contract turn-on immediate with work turn-on, *e.g.*, letter contracts with funds. Sometimes even a handshake will suffice.[41]
- DOD may need to seek teaming to balance scale and access to needed solutions. Smaller firms may not have the ability to take on funding risks for development or production that larger firms can—smaller firms may have more trouble getting rapid access to sufficient capital.
- Use Section 845 (other transaction authority) and other similar authorities that allow streamlining when this approach is attractive to non-traditional DOD suppliers or commercial firms.

The selection and ramping of the MRAP illustrates some of the challenges:

- MRAP–type vehicles existed in several firms but DOD had previously bought only a few from one firm. The Department had to quickly stand up a rapid testing program; no large-scale manufacturing existed to meet its needs.
- Smaller firms had design solutions, but did not have the scale to ramp production as rapidly as needed once the Department decided to buy MRAPs in large quantities. As a result, DOD had to seek large system manufacturers.
- Capital and risk were issues. Smaller firms extended themselves with this challenge and may end up with significant unused capacity and debt burdens.

41 Immediately prior to the first Gulf War, when Patriot units deployed to the Gulf with only two PAC-2 missiles, a handshake between senior DOD management and the prime contractor chief executive officer was sufficient to dramatically accelerate missile production well before an increased funding line had been established.

In fielding rapid response solutions, DOD will likely need to take exceptional steps to address manufacturing, training, and logistics support needs. Depending on the nature of the rapid response solution, types of providers may vary widely, as may the maturity of the product. Solution providers could range from large or small firms, to a laboratory or university, or a pure commercial source—sometimes all at the same time. The level of maturity of the manufacturing, training, and logistics support capabilities of these various suppliers could vary dramatically. DOD may find the manufacturing and support functions needed to execute a rapid reaction solution significantly overstretched.

Quick reaction solutions to capability surprises may deliver solutions so fast that organic or normalized unit or Service maintenance and repair is not possible at the outset. Planning for more than essential organic support to be available at initial fielding may slow fielding solutions. Typical requirements such as drawing packages, full normal testing, comprehensive spares, or deployed support for repairs and upgrades will need to be relaxed prior to initial fielding. Thus, the rapid response team, in concert with the Service or agency to which the solution will ultimately transition, must make decisions for the proper level of long-term DOD support. Planning is needed for initial and follow-on support, likely starting with full contractor logistics support. DOD should try to get some first order commitments, such as performance-based logistics guarantees and assurance of personnel and experience continuity, although that may be a serious problem for small suppliers. The potential for frequent rotation among contractor logistics support personnel can create a knowledge vacuum for combat soldiers, losing lessons learned and a harmful lack of expertise in the field for repairs, supply, and technical information.

Accelerated product or solution testing will likely also be needed. DOD must conduct essential performance, compatibility, and safety testing to allow fielding. However, some amount of testing and evaluation (and resulting feedback loops) may have to be performed under actual operating conditions in the field while in use. DOD will have to step in to ensure access to test ranges and environments and allow the product to be rapidly moved to the field with adequate assurance.

Surge Demands

In the past, industry has proven flexible in responding to DOD needs for rapid surge. However, DOD can improve its anticipation for capability surprise surges—an area where the Deputy Under Secretary of Defense for Industrial Policy may be able to assist. Surging places risk and capital demands on firms, which in turn often introduce delays in determining and fielding the solutions to pressing problems.

- **Providing capital for surge**. It is not unusual that when DOD needs to surge production of an existing product—such as Joint Direct Attack Munitions (JDAMs), inertial measurement units, or batteries—it may help fund creation of new capacity. But this policy is not or cannot always be implemented; rather it appears to vary by product, temporal necessity and/or setting. The use of DOD capital funding may or may not be appropriate, depending on the case, but is an area program managers need to assess carefully, particularly in dealing with smaller firms that may not have financial strength.

- **Long lead material, configuration control, sub-tier, or key technology input**. During surge, any one of these factors may set the pace for delivering capability to the field and should be tackled as soon as the solution decision is clear.

- **Priorities**. DOD response task groups should seek priority help from all possible sources, including Title III Defense Priorities and Allocation System (DPAS) ratings if needed. If programs of record are involved, those program offices' leadership chain will need to be brought on board to give priority to meet the rapid reaction response demands, which may mean that some normal program activities will at least temporarily take a back seat.

- **Training**. In many cases, DOD rapid response teams must arrange for field training teams and interim field operational support for new solutions being rapidly fielded. The field users cannot be expected to understand or deal with new solutions without support as the solution is fielded. For some types of solutions, software and network-based training could be a viable approach and less costly than having many contractors in the

field. The long-term plans for training for both operations and logistics support must be developed with the client Service to which the solution would transfer.

Appendix 3-A. Capability Assessment, Warning, and Response Office: Function and Decision-Making Process

Current analysis and decision-making related to capability surprise is fragmented across OSD, the Services, and the Joint Staff. While there is a regular pattern to strategic documents, such as the Quadrennial Defense Review and National Defense Strategy, these planning documents are too infrequent to address the scope and pace of capability change present in the increasingly fluid military operations development.

The Capability Assessment, Warning, and Response Office (CAWRO) will be a locus for surprise anticipation and assessment within DOD. It will function as an institutionalized strategic surprise management team for the Department of Defense and provide the Secretary of Defense and the Chairman, Joint Chiefs of Staff, with independent, integrative analysis of current and evolving capabilities that have the potential to become strategic or existential risks.

By using its multi-disciplinary integrative capacity, CAWRO will identify and qualify capability surprise event candidates that merit entry onto a trend watch list. Additionally, CAWRO will collect high-priority capability surprises encountered in operations. Its resident "challenge team" will also provide alternative perspectives on management options when surprise events occur.

As related to potential or actual capability surprise, the CAWRO will conduct risk, option, and program management prioritization analysis for the Secretary of Defense. Reporting directly to the Secretary, this independent status provides essential freedom of thought to challenge the status quo. Its output will be used to prioritize and resource programmatic and operational capabilities, both in response to and in anticipation of risks and opportunities.

The CAWRO's analysis and assessment activities are primarily risk assessment processes. They start with all-encompassing threat search, characterization, projection, and consequences and proceed to determine

means and actions to counter them. This process will entail option generation, prioritization, and the creation of decision packages in the presence of a great deal of ambiguity and uncertainty, and will require close coordination with key DOD and Service leadership. The CAWRO must incorporate means to test its assertions (*e.g.*, through gaming, red teaming, and community involvement) and must also be willing to hold and argue for its independent view.

The CAWRO combines the best of a knowledge management fusion center with strategic planning and risk management analysis. It champions the "seams of the defense enterprise" by anticipating multi-capability opportunities and fixing vulnerabilities. Its primary functions include:

- capability monitoring/horizon scanning
- capability projection/net assessment/competitive strategies[42]
- gathering and disseminating capability surprise experiences from operations
- risk assessment/management option analysis
- support to Secretary of Defense decision-making

The CAWRO monitors data trends in order to conduct horizon scans by blending multi-source and multi-disciplinary information and analysis. The CAWRO will employ the full range of net assessment, information, social, and intelligence tools in carrying out its mission and will work closely with the intelligence community. (Appendix 3-B provides more detail on intelligence support for the CAWRO and the proposed Rapid Response Group.)

42. Drawing on its monitoring of adversary culture, capability, and intent, and on political, demographic, and economic trends, the CAWRO can develop a series of stressing representative futures. These scenarios must then be vetted and exercised to weigh their latent risk to U.S. strategy and national existence and also their opportunities for significant unexploited U.S. advantage.

Appendix 3-B. Intelligence Support

It is critically important that the CAWRO receive both the initial intelligence picture and the corresponding threat assessment as complete and accurate as possible. It will be equally important to have a clear understanding of how the responding "entity" intends to apply and/or use that threat intelligence. The two together will frame the "capability surprise intelligence requirement." It will be of paramount importance to get this intelligence requirement right from the onset of the response process, since DOD will likely have few additional funds and, perhaps even more important, insufficient time to correct any major miscalculations or misallocations of military/industrial resources. The transition and fielding panel offers its recommendations for the nature of intelligence support for DOD surprise management, but acknowledges that it differs in form (but largely not function) from what the overall study recommends.

CAWRO Intelligence Support

Intelligence support of the CAWRO's activities would be provided by a small team of experienced, senior intelligence officers. Their primary responsibility will be to ensure that the capability surprise intelligence requirement is as complete and accurate as possible. In addition, their responsibilities will include working with the national intelligence community to develop and maintain an appropriate anticipatory intelligence detection process and over-the-horizon early warning system for possible future capability surprises. The intelligence cadre assigned to the CAWRO will have the analytical skills and experiences to plan and direct national-level intelligence collection operations. One member of the CAWRO intelligence cadre would serve as the senior intelligence officer for the Rapid Response Group, ensuring that the appropriate national and operational intelligence support is being provided to each rapid response team.

The Applied Intelligence Support Team(s)

Once the nature and urgency of the "capability surprise" has been determined and the Secretary of Defense has decided on the response option(s), an appropriate applied intelligence support team will be formed to work with the new rapid response team. The applied intelligence support team, varying from six to twelve members, would include, as appropriate to the nature of the surprise:

- senior national and operational intelligence officers
- an experienced, all-source intelligence collection manager with the authority to task both the national and operational collection systems
- senior intelligence analysts, experienced in conducting threat assessments, options analysis, and scenario development
- science and technology intelligence analysts with both weapons and industrial assessment experience
- an expert in open source intelligence, capable of fully exploiting the business intelligence community
- an expert in red teams and war gaming

The applied intelligence support team would become an integral part of the rapid response team, ensuring that the CAWRO's initial intelligence assessment and threat-model are properly transferred and incorporated into the response teams follow-on efforts. The applied intelligence team will then ensure that the "capability surprise" intelligence assessment and threat model are kept up-to-date throughout the transition and fielding phase of the DOD response.

Depending upon the outcome of the initial intelligence review, an all-source national intelligence community collection plan would be developed and levied on national and operational intelligence collection authorities. This will include the traditional indicators and warning, as well as new horizon-scanning early warning systems. In addition, government directed open-source collection and, as appropriate, private sector business intelligence resources will be used. Technology scouts would also be employed, to collect business intelligence for the response

group and its contractors; the scouts would also be on the lookout for possible enemy efforts to acquire similar business intelligence.

The applied intelligence team's analytical cadre will be responsible for organizing and leading a variety of *ad hoc* assessment efforts. These analytical efforts would include:

- Maintaining and enhancing the initial threat-model(s), ranging from paper studies to simulations, including the possible acquisition and live use of actual threat equipment and/or technology. This effort would also include the creation of future and/or alternate threat scenarios.
- Developing and using risk assessment methodologies to evaluate surprise-response options.
- Net assessments, including both net technical and operational assessments, designed to identify both threat and response vulnerabilities. The net technical assessment outputs would also support development of response countermeasures.

The applied intelligence team would support, and as appropriate, lead red team activities. These efforts will stress the acquisition and use of authentic threat strategy intelligence and equipment as well as finding threat-experienced players to participate. Using the red team's experience, the applied intelligence team will help develop several professionals, similar to the Army's "new" red team players, who can serve as "intelligent advisors" to the response team's operational planning and counter-threat response effort.

The applied intelligence team would assist in the preparation and conduct of "capability surprise war games" for the response team(s). This war game capability will be kept up-to-date and used initially to test the appropriateness and effectiveness of the response team's planned solution; intelligence gaps and collection priorities would also be identified. This war and/or operational gaming capability would be maintained for use throughout the transition and fielding process.

The most complete and up-to-date threat models would be used in the "final" war game to assist in the development of the response team's rollout plan. The results of this war game would include contingency

plans to cope with possible enemy reactions. The applied intelligence team would develop and put in place an intelligence collection and reporting plan to monitor possible enemy responses to the response team's initial field activities, which would include indications and warning trigger indicators for the prepared contingency plans.

The applied intelligence team will support the rapid response team's contractors throughout the research, development, test, and evaluation process. Contractor requirements for intelligence inputs and support will have the highest priority. Denial and deception efforts will be included from the onset, factored into both intelligence and response research and development activities at every stage, including war gaming. As mentioned previously, the creation and use of Army red team "intelligent advisors" will be made available from design to actual rollout of the response capability.

Lastly, a field operations intelligence support capability would be created and put in place by the applied intelligence support team, including some of its own team members as appropriate. In addition to maintaining the "capability surprise" threat model, the new team's responsibilities would include: 1) supporting future response enhancements and countermeasure development; 2) developing and executing national intelligence and operational collection plans; and 3) providing red team and war gaming experience and advice. This effort is aimed at ensuring the most effective transfer of intelligence capabilities and experience to those responsible for the field operations of the CAWRO's response to capability surprise.

Appendix 3-C. Rapid Response Operating Concept

Once the Secretary of Defense decides to create a rapid response team based on input from the CAWRO, the Secretary will issue a directive package setting forth the tasking to the team, together with associated responsibilities and authorities. The directive would also lay out ground rules for support from DOD staff and components. The tasking would set a target fielding date and provide initial funding to further refine a plan of action for the rapid response team, including technical approaches, execution funding and resource needs, milestones, a fielding plan, and transition plans at the end of the project. Reporting and review structure and frequency would also be defined.

Proposed Functions in the Rapid Response Group

As envisioned by this panel, the Rapid Response Group would have the ability to support individual rapid response teams as directed by the Secretary of Defense. In order to perform this function, the Rapid Response Group must develop a qualified rapid response team candidate leader roster, a database ("Rolodex") of sources of expertise, access to funding, acquisition and contracting authority, personnel management, and tasking skills.

Qualified candidate leader roster. The Rapid Response Group will maintain a roster of potential rapid response team leaders. These potential leaders will be competitively selected and maintained on a rotating roster. When a team is chartered, the Rapid Response Group will recommend a rapid response team leader to the Secretary of Defense for approval and tasking. Rank (military or civilian), expertise, and, perhaps most critical, leadership skill and commitment should be considered in making this recommendation. Although availability also must be a consideration, given the priority of this activity, availability should not generally depend on ongoing commitment to a lower priority activity. Selection to lead (and subsequent success in carrying out the assigned

mission) should be considered a significant career accomplishment, analogous to successful performance on a combatant command Commander's Action Group. In this instance, a leader might be identified as a member of the "Secretary of Defense's Action Group," with high potential for promotion.

"Rolodex" of sources of expertise. The Rapid Response Group will maintain a roster of experts in various technical and operational disciplines and in organizational management. Once a team is chartered and a team leader assigned, this database becomes available to the team leader to draw on for recruiting or tasking needed expertise.

Funding. Funds to establish and ramp up rapid response team activities will be maintained in an appropriated and authorized account that will be renewed in each annual appropriation. The nominal size of this account will be on the order of $200 million, which should be adequate to conduct the first few months of activity by a team, while additional funds are made available. Funding for rapid response teams should extend over the life of the project and be "colorless" (unrestricted) money.

Acquisition authority. The rapid response teams, through the Rapid Response Group, will have authority to develop, procure, and support materiel items under expedited rules until they are handed over to the "normal" acquisition and support systems of the appropriate Service or agency at the conclusion of the project.

Contracting authority. The Rapid Response Group will include very experienced contracting officers and staff who have specific expertise and training needed to execute high-priority, streamlined, fast-tracked contracts. They will appropriately distribute risk between contractors and the government while protecting the government's interests, but without delaying implementation of urgently needed solutions.

Hiring authority. Most members of rapid response teams will be drawn from existing DOD rolls, but there will also likely be expertise that will need to be drawn from other sources, including Intergovernmental Personnel Authority (IPAs), consultants, and temporary hires. The Rapid Response Group should have the in-house capability to support its teams with expedited human resource support.

Tasking authority. The Rapid Response Group should have the ability to task other DOD organizations to support rapid response teams under the authority of the Secretary of Defense.

Streamlined oversight. The Rapid Response Group will arrange for appropriate oversight of each rapid response team, but the model must be based on streamlined management oversight of critical elements and timelines to allow the fast pace of the project to proceed unhampered.

Composition and Management Approach of the Rapid Response Teams

The rapid response teams are envisioned as being "Skunkworks-like" in terms of expertise and management philosophy. They should be small and agile compared to standard program organizations, work very closely with industry, and be relatively free from outside interference and review. The team should have contracting and other support from the Rapid Response Group, a strong systems engineering function, user representation, and representation from the organizations the project will transition to for sustained production and support. Teams will be tailored to the task being implemented, which could range from small numbers of new prototypes, to modifications of existing systems, to large-scale serial production.

End Date/Transition to Mainstream Support

The Rapid Response Group and the rapid response teams are not intended to replace the existing development, acquisition, and support structures of the Department. The sole purpose of this structure is to jump-start responses to urgent high priority surprise threats or to address unforeseen risks and vulnerabilities in an urgent way. Every rapid response team will have a pre-established end date or transition plan to move any material solutions into the appropriate "normal" acquisition and support system. This should happen as soon as regularly budgeted funds can be applied, generally within no more than two years of the team's formulation. To facilitate this transition, the leadership, staff, and other support for the rapid response team should be drawn, in part, from the organization that would logically "receive" responsibility for the project.

Appendix 3-D. Challenges for Rapid Software Transition and Fielding

Software, either in the form of a surprise originating in software or in using software to adapt to a surprise, presents a different set of challenges from hardware. These challenges stem from the diversity of types of software and responses to surprises, the nature of intellectual property, the scale of the response, the size of the company assisting with the response, and the appropriate programming style. Existing rapid acquisition cycles appear neither to consider usability nor to anticipate larger needs. The potential for software surprise can be expected to grow as the demand for collaboration and virtualization software applications—such as e-mail, chat, Google™, Wikipedia, social networking—proliferates and these applications are adopted into DOD culture. This type of software will require a different style of transition and fielding as the code will likely be open source, provided by small startups either owned by foreign governments or staffed with foreign nationals. It may be provided through the Software as a Service paradigm.

Four Types of DOD Software and Impact on Rapid Response

DOD software can be divided into four broad categories: real-time embedded control; command, control, communications, and intelligence (C3I); information systems; and network applications. The first three categories represent "traditional" DOD software applications such as accounting, logistics tracking, and schedule management purchased by well-understood methods, while the fourth category captures the rapidly emerging software used or spontaneously downloaded from the Internet or wireless networks (*e.g.*, email, chat, blogs, text messaging, Google™, Wikipedia). Responding to a software surprise in the traditional categories is generally a straightforward patch or extension of an existing contract. Responding to a surprising new network-centric application is more difficult as the application may be open source, created by a small start-up reluctant to work with the DOD or having foreign nationals/ investors, and may involve risk and evolutionary acquisition.

In order to understand the differences and difficulties in responding to software surprises, it is helpful to compare the four types of software on three dimensions. The first dimension is the **scale of the software** being created. The scale of the software can be considered as a spectrum spanning: 1) a refinement patch or tweak to existing software; 2) a major modification with formal, detailed requirements; or 3) a spiral development/evolutionary process because needs are not well-understood, cannot be fully met with the first instantiation, or rely on a measure-countermeasure cycle of response in which new surprise/response is anticipated. The second dimension is **programming style**, which can range from customized code written solely for the application and is owned by DOD, to proprietary code that is purchased and adapted for DOD, to proprietary code that is downloaded or used for a small fee, to open source which is downloaded or used. The third dimension is the **size of the company**. The size of company ranges from a large defense contractor, to a software house or developer, to a start-up company.

Real-time embedded control software (e.g., vehicle control) and **C3I software** (e.g., missile warning and attack assessment) are generally produced by a defense contractor or specialized "captive" supplier writing customized code, with all intellectual property belonging to DOD. **Information systems software** (e.g. accounting and planning) are usually purchased (with some modifications) from a large software developer such as Microsoft® or Oracle® who retains the intellectual property. In contrast, **social network-centric application software** is often produced by small start-up companies who have no reserves of programmers to be diverted to work on DOD requests or may fear losing intellectual property rights. These start-ups may have considerable foreign investors or employ foreign nationals.

The scale of the response to a surprise suggests that there are three clusters of responses (Figure 3-D-1). Surprises involving real-time embedded control and C3I software are likely to be either a patch or a new set of requirements (*i.e.*, a new application). This is a cluster where the core software undergoes a well-described **DOD-specified extension**. Surprises with information systems may also be handled with a patch but significant modifications may require working cooperatively with the vendor. For example, the vendor may resist branching their product into a commercial version and a DOD version

or the vendor (not DOD) may be the expert who should generate the new requirements. In general, information system vendors are generally large enough to have a government-oriented division, and employees and practices appropriate for handling sensitive software. As a result, this cluster is where the core software undergoes **vendor-generated extensions**. The third cluster is the most challenging, as it captures the unknown process of working with network-centric applications in a **cooperative, spiral development process** to either modify an existing product or create a new, related product. Here, the companies are small, may not have resources to work with the government, and cannot afford delays in contracting or negotiating intellectual property rights. DOD may be uncomfortable with open source code or open application programming interfaces (APIs) to proprietary code. DOD may be able to have its own personnel add or modify the code.

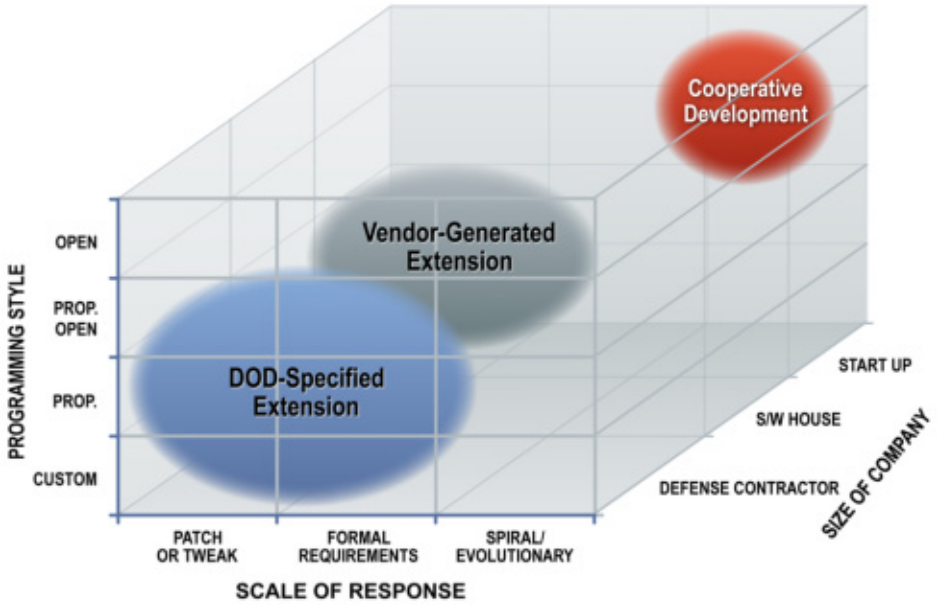


Figure 3-D-1. Three Types of Responses to Software Surprises

The difference between the three types of responses to the surprise is more significant if considered from a software engineering and usability perspective. In the two extension approaches, a top-down specification of the solution is presumed. That is, the problem and the desired (approximate) solution have been determined. However, in the cooperative development approach, the solution is bottom-up—that is,

the solution bubbles up through analysis, discussion, and even experimentation, to iteratively develop a solution. In the extension approach, usability may not be a concern. (Usability measures the acceptability of the user interface and human factors, the reliability of the software, and aspects such as degree of difficulty in installing and maintaining the software.) Real-time embedded control and C3I software concentrate on "invisible" functionality, so usability is not a prime issue. Information systems are intimately concerned with usability as part of their market competitiveness. Network-centric applications are highly usability oriented. The ability to quickly install them, having intuitive interfaces, and showing reliability are the distinguishing features that lead to market dominance.

Removing Barriers to Responding Quickly to Software Surprise

There is precedent for quickly instigating DOD and vendor-generated extension responses. But, unfortunately, there are several barriers to cooperative development of social network-centric applications, and barriers to successful use of these software applications. These barriers can be addressed by giving the rapid fielding office the appropriate authority and by putting in place sufficient usability and security testing.

The historical requirements that hamper small information technology companies and create barriers to the rapid response to software surprises are:

- **Loss of intellectual property rights, proprietary software, and concerns pertaining to International Traffic in Arms Regulations (ITAR).** Social networking software companies are unlikely to give up intellectual property rights or write DOD-only code, as their success depends on the fastest, widest distribution of functionality possible. Likewise, as the software industry moves to "software as a service" applications that are accessed over the Internet on demand, it is unrealistic for DOD to own the code. The time spent negotiating intellectual property rights is often significant and expensive. The rapid fielding office should be aware of these situations; have thought out a spectrum of possible responses and created

alternatives to cumbersome intellectual property agreements; and be prepared to offer reasonable compensation for DOD-only features or accept the incorporation of such features into the vendor's product. ITAR that stipulate guidelines on importing and exporting software also present barriers.

- **Unclear or competing standards.** Incomplete or conflicting architectures and standards, such as Joint Architecture for Unmanned Systems, may interfere with desired functionality and timely development, and also intimidate smaller companies that do not have the manpower to attend meetings or lobby for changes. The rapid fielding office should serve as a liaison and arbiter between the company and the standards agency.
- **Imposition of clearances.** Clearances may be a problem even if the company is in the United States. The company may have a large number of foreign employees, use international development teams, be partially owned by a foreign company, and/or have foreign investors. It may not be realistic for the rapid fielding office to enforce "keeping the genie in the bottle" through security clearances. Also, small companies cannot afford the costs, distractions, and reallocation of manpower to handle splitting their company into secure and open projects.
- **Lack of acceptance of risk and initial failure.** Addressing a surprise in social-network software may require a radical new capability in a short time frame and may result in a move-countermove series with adversaries. This suggests that the development cycle will be iterative or evolutionary—the first solution may not work or may be quickly neutralized. Therefore, the office should be prepared to deal with an ongoing development cycle.

It should be noted that, in some sense, the rapid acquisition of social network-centric software may follow U.S. Special Operations Command acquisition processes where the command is allowed to negotiate lower prices for development of equipment in return for the company being able to either sell the equipment openly or advertise that it is being used by the command.

While waiving **usability** and **software security** requirements appear to reduce barriers to effective response, this approach may not necessarily lead to desired results. Usability and software testing are generally waived in rapid acquisition processes in the mistaken assumption that this speeds up the process and that "something is better than nothing." Though subtle, a poor user interface or human factors may do more harm than good. Likewise, security vulnerabilities may obviate any utility of the software and open up the larger enterprise to additional attacks. Since usability is key in the acceptance and effectiveness of social network-centric software, streamlined usability testing should be incorporated into the rapid acquisition process. Testing for unintended consequences and compatibility must also be done. Funding for research and development for specific techniques may be necessary.

Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

MAY 15 2008

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board (DSB) 2008 Summer Study on Capability Surprise

The United States (U.S) is in a never-ending race to maintain a capability edge against potential opponents. Despite significant U.S. science and technology prowess, numerous paths exist for adversaries to achieve "capability surprise." Many of the alternative paths for adversary capability development do not rely on leading edge science and are sometimes achieved at a significant cost advantage over U.S. capabilities. Fortunately, capability development paths exist without using cutting edge science and technology for the U.S. and may also create opportunities for the U.S. to employ cost imposing strategies on adversaries.

There are three different scenarios in which capability surprise can occur:

1. Surprise in the laboratory. Although less likely than some other forms of surprise due to the extensive intellectual interchange and competition among laboratory scientists, surprise from a fundamental scientific breakthrough is still possible. Breakthroughs in mathematics, algorithms, cryptography, and device technology, for example, can spring from anywhere. More likely are the surprises that might result from the clever first application(s) of scientific discoveries.

2. Surprise during transition from concept to fielded product. Transition time is affected by numerous issues, including: bureaucratic process, manufacturing capability, training, and logistics. Presuming we all share the same worldwide base of science, whoever can move it into fielded weapons systems the fastest has a real advantage – and some countries have the resources, agility, and will to accomplish this. An adversary that cares less about process, cost, and potential abuse and more about speed has the potential to get capabilities to the field more rapidly than we might expect. Furthermore, the spread of manufacturing technology, service and process improvement techniques, and management knowledge make the transformation of laboratory knowledge into reliable, repeatable, deliverable, maintainable equipment more likely. Globalization accelerates market workforce training and will accelerate the development of this capability as other countries compete in the global market.

3. Surprise introduced by the unconventional or unforeseen use of an existing capability. It might be commercial (e.g., the Internet as a command and control net) or a weapons system (e.g., the B-52 in a tactical support role). Innovative development of new capability using existing force structure can be extremely rapid, prove costly in combat, and be extremely effective. Another facet of this particular surprise mechanism is the employment of old or low technology against high-end U.S. capability.

Underlying the kinds of surprise are the reasons why surprise may occur. A partial list of such reasons includes:

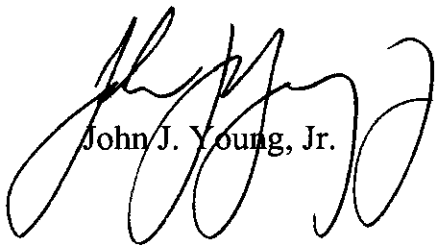
a. Failure to respond to the introduction of a new capability
b. Planned response proceeds at too leisurely a pace
c. Failure to imagine a capability
d. Underestimating an adversary's prowess to introduce a capability
e. Assuming that an adversary would not dare to do such a thing

The study should focus on the *whats* and *whys* of capability surprise and the measures to ensure that DoD and its interested partners are best positioned to prevent, or mitigate, capability surprise against itself. It should assess the surprise mechanisms, dealing with how surprise may occur, and develop relevant recommendations in two domains: how to reduce the potential for surprise across the dimensions outlined above; and given that some surprise will always occur, how to better prepare ourselves to respond appropriately. Recommendations should also be formulated for ensuring that the Department, in coordination with the intelligence community, has both the people and processes in place not only to identify potential surprises across the dimensions outlined above but also, on an annual basis, to formally assess both risks and opportunities in dealing with them.

Finally, the study should assess cost-imposing strategies to include what adversaries may do to the U.S. and what the U.S. could do against potential adversaries, both with respect to high-end technology solutions and employment of low-end or old technology solutions. As part of this assessment, the study should also consider how the U.S. might impose surprise on its adversaries in rapid, cost effective, and unique ways.

The study will be co-sponsored by the Under Secretary of Defense for Acquisition, Technology and Logistics, the Under Secretary of Defense for Intelligence, the Vice Chairman of the Joint Chiefs of Staff, and the Commander, Joint Forces Command. Dr. Miriam John and Mr. Robert Stein will serve as Chairpersons of the Summer Study. Mr. R.C. Porter of OUSD(I) and Mr. Robert Baker of the Office of the Director of Defense Research and Engineering will serve as co-Executive Secretaries; and Lieutenant Colonel Chad Lominac, USAF, will serve as the DSB Secretariat Representative.

The Task Force will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of section 208 of title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.



John J. Young, Jr.

Study Membership

NAME	AFFILIATION
Chairs	
Miriam John	Private Consultant
Robert Stein	Private Consultant
Executive Secretaries	
Bob Baker	OSD/DDR&E
R.C. Porter	OSD/USD (I)
Senior Advisors	
Craig Fields	Private Consultant
John Foster	Private Consultant
Ted Gold	Private Consultant
George Heilmeier	Private Consultant
Bill Schneider	International Planning Services, Inc.
Vincent Vitto	Private Consultant
Challenge Panel	
Chair	
Gerry Yonas	Sandia National Laboratories
Members	
Bob Atkins	MIT
Roy Evan	MITRE
John Foster	Private Consultant
Rich Haver	Northrop Grumman Corp.
Ron Kerber	Private Consultant
Larry Lynn	Private Consultant
Joe Markowitz	Private Consultant
Jason Webster	Northrop Grumman Corp.
Institutional Process Change Panel	
Chair	
Joseph Braddock	The Potomac Foundation
Members	
George Cybenko	Dartmouth University
Bruce Deal	SET Corporation
Jacques Gansler	University of Maryland
Ted Gold	Private Consultant
Michelle Van Cleave	NDU
Technology Panel	
Chairs	
Zach Lemnios	MIT Lincoln Laboratory
Jim Shields	Draper Laboratory

NAME	AFFILIATION
Members	
Melissa Choi	MIT Lincoln Laboratory
Frank Fernandez	Private Consultant
Jim Gosler	Sandia National Laboratories
Anil Jain	Michigan State University
Steve Kornguth	University of Texas at Austin
Mark Lister	StratTechs, Inc.
Len Polizzotto	Draper Laboratory
Robert Popp	National Security Innovations, Inc.
Ron Sega	Colorado State University
Ann Marie Skalka	Fox Chase Cancer Center
Robert Tenney	BAE
Jim Thomas	Applied Minds, Inc.
Joe Walkush	SAIC
David Whelan	The Boeing Company
Government Advisors	
Jack Bell	L&MR
Mel Currie	NSA
Matt Hosey	NGA
Steve Thompson	DIA
Operations Panel	
Chairs	
Michael Hagee	Private Consultant
James McCarthy	USAFA/DFPS
Members	
Eric Evans	MIT Lincoln Laboratory
Greg Gardner	Oracle Corporation
Thomas Hammes	Private Consultant
John Hanley	Institute for Defense Analyses
John Hawley	Near Space Systems, Inc.
David Johnson	RAND Corporation
Jim Kurtz	Institute for Defense Analyses
James Lacey	Institute for Defense Analyses
Dawn Meyerreicks	Private Consultant
Dave Nichols	Private Consultant
Ron Sega	Colorado State University
Thomas Steffens	FLIR Systems Inc.
Bill Studeman	Private Consultant
Patrick Toohey	Sullivan Haave Associates
John Vines	Private Consultant
Linton Wells	National Defense University

NAME	AFFILIATION
Government Advisors	
R.C. Porter	OSD/USD (I)
Andrew Roberts	DIA
Transition and Fielding Panel	
Chairs	
Christine Fisher	Private Consultant
Bill Howard	Private Consultant
Members	
Dave Drumheller	ONR
Regina Dugan	Dugan Ventures
Ed Franklin	Private Consultant
Matt Ganz	Phantom Works
Jan Herring	Herring and Associates LLC
Frank Kendall	Private Consultant and Attorney at Law
Ira Kuhn	Directed Technologies, Inc.
Bob Lucky	Private Consultant
Robin Murphy	Texas A&M University
Harry Raduege	Deloitte and Touche LLP
Joseph Santarelli	Booz Allen Hamilton
Leigh Warner	Private Consultant
Government Advisors	
Mark Mandeles	RRTO/Emerging Capabilities Division
Additional Government Advisors	
Russell Buttram	U.S. Marine Corps Strategic Initiatives Group
Daniel Flynn	ODNI
Garth Jensen	OPNAV N81
Chuck Kimzey	U.S. Pacific Command
Don Wurzel	Arete Associates
Cecelia Phan	Joint Staff J6CTO
Steve Smith	HDQA G-3/5/7
Randy Tebbing	OUSD (I) CAMM
DSB Representatives	
Brian Hughes	DSB Executive Director
Charles Lominac	U.S. Air Force Military Assistant
Karen Walters	U.S. Army Military Assistant

NAME	AFFILIATION
Staff	
Barbara Bicksler	Strategic Analysis, Inc.
Rebecca Bortnick	Strategic Analysis, Inc.
Greg Byerly	Strategic Analysis, Inc.
Tim Cullen	Strategic Analysis, Inc.
Kelly Frere	Strategic Analysis, Inc.
John Fricas	Strategic Analysis, Inc.
Marcus Hawkins	Strategic Analysis, Inc.
Amy Hoang-Wrona	Strategic Analysis, Inc.
Jennifer Howell	Strategic Analysis, Inc.
Brian Keller	Strategic Analysis, Inc.
Teresa Kidwell	Strategic Analysis, Inc.
Toni Marechaux	Strategic Analysis, Inc.
Diane O'Neill	Strategic Analysis, Inc.
Ted Stump	Strategic Analysis, Inc.

Presentations to the Study

NAME	TOPIC
Plenary Sessions	
April 29, 2008	
Mr. Jeff Green Office of General Counsel, Office of the Secretary of Defense	Standards of Conduct
Mr. Ben Riley Director, Rapid Reaction Technology Office of the Director, Defense Research and Engineering (DDR&E)	Defense Policy Implications of Global Technology Trends
Mr. Andy Marshall Director, Net Assessment	Discussion on Capability Surprise
May 1, 2008	
Gen James Cartwright, U.S. Marine Corps Vice Chairman, Joint Chiefs of Staff	Discussion
Dr. Steve Chiabotti and Dr. Everett Dolman School of Advanced Air and Space Study, Maxwell Air Force Base	Theory of Capability Surprise
Mr. Larry Burgess Deputy Under Secretary of Defense for Collection and Analysis Mission Management	Discussion
May 19, 2008	
Staff, Central Intelligence Agency	Intelligence and Science and Technology Perspectives
Mr. Al Shaffer Principal Deputy Director of Defense Research and Engineering, Office of the Secretary of Defense	DDR&E Perspectives
Mr. Dan Flynn Deputy Director of National Intelligence for Analysis	Analysis Perspectives
May 21, 2008	
Mr. James Johnson Program Analysis and Evaluation, Office of the Secretary of Defense	Shaping the Pacific Region
Dr. Thomas G. Mahnken Office of the Under Secretary of Defense for Policy	Discussion

NAME	TOPIC
June 10, 2008	
Mr. Adam Nucci DDR&E	Global Emerging Technologies Study
Mr. Art Zuehlke Defense Intelligence Agency	Defense Intelligence Agency Perspective
Dr. Ruth David ANSER	Avoiding Surprise in an Era of Global Technology Advances
June 12, 2008	
Dr. Melissa Flagg	ONR Global
Mr. Chris Bannon	Navy Deep Red
Mr. George Spix	Microsoft Experience
June 25, 2008	
Dr. Anita Jones Former DDR&E	Information Technology Capabilities
Dr. Tony Tether Director, Defense Advanced Research Projects Agency (DARPA)	DARPA Perspectives
Mr. Christopher Darby CEO In-Q-Tel	Discussions
LTG John R. Wood, USA Deputy Commander, Joint Forces Command	Joint Forces Command Perspectives
Dr. Dave Johnson, RAND and Mr. Jim Lacey, IDA	Discussions
June 26, 2008	
General Anthony Zinni, USMC (Ret) and Ambassador Richard Armitage	Discussions
June 27, 2008	
Ambassador Kenneth Brill Director, National Counter-proliferation Center (NCPC)	NCPC Perspectives
LTG Thomas Metz, USA Director, Joint Improvised Explosive Device Defeat Organization (JIEDDO)	JIEDDO Perspectives
Dr. Don Kerr Deputy Director of National Intelligence	Discussions
July 22, 2008	
Dr. Jim Heath National Security Agency (NSA) Science Advisor	NSA Perspective

NAME	TOPIC
Mr. Frank Cappuccio	Lockheed Martin Skunk Works
July 23, 2008	
Andy Nicholson Senior Programme Leader, Dstl Farnborough, UK	An Allied Perspective
July 24, 2008	
Mr. Nick Marsella Co-Director, U.S. Army University of Foreign Military and Cultural Studies	Army Red Teaming
Dr. James Tegnelia Director, Defense Threat Reduction Agency	Discussion
Mr. Mike Leiter Director, National Counterterrorism Center (NCTC)	NCTC Perspective
Operations Panel	
May 2, 2008	
VADM Dave Nichols	Master 4GW Brief
July 23, 2008	
Frederick Brosk Office of the Under Secretary of Defense for Intelligence	Capability Surprise
Technology Panel	
June 26, 2008	
Dr. William S. Rees, Jr. Deputy Under Secretary of Defense (Laboratories and Basic Sciences)	Overview of Relevant Basic Science in DOD
Mr. Bill Linton CEO, Promega	Global View from the Biotech Industry
July 22, 2008	
Dr. Mark M. Little, Senior Vice President and Director, GE Global Research	Discussion on GE Corporate Strategies
July 23, 2008	
Mr. Gregory D. Gordon National Ground Intelligence Center Mr. Paul Parmiter, IMC Dr. Dewey Murdick National Ground Intelligence Center	Discussion on TechWatch
Transition and Fielding Panel	
May 20, 2008	
Mr. Damon Walsh Executive Vice President, Force Protection industries, Inc.	Mine Resistant Ambush Protected (MRAP) Industry Perspective

NAME	TOPIC
Mr. Paul Mann Program Manager MRAP Mr. Barry Dillon Executive Director, MARCORSYSCOM Mr. Will Randolph Assistant Commander for Contracts	MRAP Government Perspective
June 11, 2008	
BG Fox, J8 Office	Joint Urgent Operational Needs Statement, Joint Rapid Acquisition Cell
Dr. Edward Turano Director, Nuclear Technologies Directorate	DOD Research and Development to Counter the Threat from Lost, Stolen and Improvised Nuclear Weapons
June 26, 2008	
Dr. Lin Wells National Defense University	Trends and Shocks
Ms. Kathleen Harger Assistant Deputy Under Secretary of Defense for Innovation and Technology Transition	USD (AT&L) Strategic Initiative on Innovation and Technology Transition
LTC Nick Wager, JDI	Weapons of Mass Destruction/Terrorism
Gen (R) Montgomery Meigs	JIEDDO and WWI Subs
July 23, 2008	
Col. Bishop Director Rapid Equipping Force Mr. Gerald Ferguson Deputy Director, U.S. Army Rapid Equipping Force	Rapid Equipping Force (REF)
Dr. Alok Das Director, Air Force Research Lab, Core Process 3	Air Force Research Lab Core Processes 3
Dr. Leo Christodoulou Defense Sciences Office, Defense Advanced Research Projects Agency	WASP & HARDWIRE
Mr. Mike Knollman Assistant Deputy Under Secretary of Defense for Joint & Coalition Operations Support	Joint and Coalition Operations Support

Glossary

ADUSD (I&TT)	Assistant Deputy Under Secretary of Defense for Innovation and Technology Transition
AFSSS	Air Force Space Surveillance System
AEHF	advanced extremely high frequency
ARPA	Advanced Research Projects Agency [now DARPA]
ASB	Army Science Board
B-2	stealth bomber
B-52	Stratofortress (strategic bomber)
BRIEM	Belarus Research Institute for Epidemiology and Microbiology
BWC	Bacteriological and Toxic Weapons Convention
C3	command, control, and communication
C3I	command, control, communication, and intelligence
CAWRO	Capability Assessment, Warning, and Response Office
CDR JFCC SPACE	Commander, Joint Functional Component Command for Space
CENTCOM	United States Central Command
CEO	chief executive officer
CERN	European Organization for Nuclear Research
CJCS	Chairman, Joint Chiefs of Staff
CNN	Central News Network
COCOM	combatant command
COTS	commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency
DaVenCi	Defense Venture Catalyst Initiative
DDR&E	Director of Defense Research and Engineering
DIA	Defense Intelligence Agency
DIAP	Defense-wide Information Assurance Program
DNI	Director of National Intelligence
DOD	Department of Defense
DOTMLPF	doctrine, organization, training, material, leadership and education, personnel, and facilities
DPAS	Defense Priorities and Allocation System
DSB	Defense Science Board
Dstl	Defense Science and Technology Laboratory (United Kingdom)
EW	electronic warfare

GE	General Electric
GPS	Global Positioning System
HALE	High Altitude Long Endurance
HMMWV	High Mobility Multipurpose Wheeled Vehicle
HO IX	Horton HO IX V2 (GO229)
IARPA	Intelligence Advanced Research Projects Activity
IDA	Institute for Defense Analysis
IED	improvised explosive device
IGY	international geophysical year
IMU	inertial measurement unit
IPA	Intergovernmental Personnel Authority
ISP	Internet service provider
ISR	intelligence, surveillance, and reconnaissance
ITAR	International Traffic in Arms Regulations
JCIDS	Joint Capabilities Integration and Development System
JDAM	Joint Direct Attack Munition
JFCC	Joint Functional Component Command
JFCC SPACE	Joint Functional Component Command for Space
JIEDDTF	Joint Improvised Explosive Device Defeat Task Force
JIEDDO	Joint Improvised Explosive Device Defeat Organization
KMT	Kuomintang
MILSTAR	Military Strategic and Tactical Relay
MRAP	Mine Resistant Ambush Protected (vehicle)
MURI	Multidisciplinary University Research Initiative
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NGIC	National Ground Intelligence Center
NSA	National Security Agency
NSSI	National Security Space Institute
ODDR&E	Office of the Director of Defense Research and Engineering
ODNI	Office of the Director of National Intelligence
ODUSD (IP)	Office of the Deputy Under Secretary of Defense for Industrial Policy
OECD	Organisation for Economic Cooperation and Development
OIF	Operation Iraqi Freedom
ONR	Office of Naval Research
ORS	Operationally Responsive Space

OSD	Office of the Secretary of Defense
PAC-2	Patriot Advanced Capability-Two
PC	personal computer
PNT	position, navigation, timing
R21	Cryptographic Research and Design Division (in the National Security Agency)
R&D	research and development
RAFO	Rapid Acquisition and Fielding Organization
RAIDRS	Rapid Attack Identification Detection and Reporting System
REF	Rapid Equipping Force
RLM	Reich Air Ministry (of the German government)
S3	Social Software for Security
S&T	science and technology
SATCOM	satellite communication
SBIRS	Space Based Infrared System
SBSS	Space-Based Surveillance System
SBV	Space-Based Visible
SETI	Search for Extraterrestrial Intelligence
SLA	service level agreement
SM-3	Standard Missile-Three
SOCOM	United States Special Operations Command
SOV	statement of vulnerability
SSA	space situational awareness
SSBN	ballistic missile submarine
TacSat-2	Tactical Satellite Experiment
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD (I)	Under Secretary of Defense for Intelligence
USMC	United States Marine Corps
USSTRATCOM	United States Strategic Command
VLSI	very large-scale integration
WGS	Wideband Global SATCOM
WTO	World Trade Organization